The GDPR, a game changer for electronic identification schemes? The case study of Gov.Verify UK

Sophie Stalla-Bourdillon (University of Southampton), Henry Pearce (University of Portsmouth), Niko Tsakalakis (University of Southampton)

Abstract

This article constitutes an interdisciplinary analysis of the UK Government's electronic identification system, GOV.UK Verify, and its compatibility with some important aspects of EU data protection law. Through an in-depth examination of the technological architecture of the GOV.UK Verify service, as well as some of the most significant constituent elements of both the Data Protection Directive and the imminent General Data Protection Regulation – notably the legitimising grounds for the processing of personal data and the doctrine of joint controllership – the article highlights several flaws inherent in the GOV.UK Verify's development and mode of operation, and advances the argument that it is incompatible with some major substantive provisions of the European Data Protection Framework. Other issues, such as potential incompatibilities between the terms of the General Data Protection Regulation and other associated pieces of legislation – notably the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market – can be reconciled are also considered.

1. Introduction

The General Data Protection Regulation (GDPR)[1] was adopted by the European Union (EU) on 24th May 2016 will become applicable from 25 May 2018. It is intended to be a game changer for businesses operating within, or simply targeting, the EU Digital Single Market. Pursuant of this, we are now seeing the emergence of startups all over Europe promising to help businesses adapt to the evolving legal framework. Bigger companies have also been eager to invest in staff training as well as compliance assurance mechanisms and processes. The strengthening of the arsenal of punitive sanctions for breach of its terms largely explains why the GDPR has been under the spotlight since its adoption.

Whether the GDPR should be seen as a regulatory revolution has been heavily debated by various observers since the beginning of its legislative process in 2012. It is undeniable for instance, that the roots of many of the GDPR's substantive provisions can be traced to prior legislative instruments, notably the Data Protection Directive (DPD), which was adopted in 1995.[2] Nevertheless, the GDPR coming into force will mean that many organisations that are already complying with the terms of the DPD will be required to modify some of their practices in order to remain compliant with various substantive tenets of the European data protection framework. This is particularly true in respect of mechanisms and procedures relating to data subject rights, as the list of rights contained in the GDPR is more expansive than that found in the DPD. However, there are also questions that can be asked in respect of the GDPR's other notable provisions. Have, for instance, the rules relating to security measures that must be implemented by data controllers evolved as well? What about the rules regarding restrictions concerning the choice of appropriate legal bases by which personal data processing activities can be legitimised?

As is the case under the outgoing DPD, the GDPR applies to public authorities. As alluded to above, most of the scholarly attention has focused on the implications of private actors having to comply with GDPR standards. Much less, however, has been written about the regulatory burden the GDPR imposes upon public authorities. This is perhaps surprising, as many Government services are underpinned by daily personal data processing activities and, on occasion, such services can be seen to transfer personal data to third parties for the performance of secondary activities, such as conducting research.

Significantly, just like private sector institutions, public authorities can also be faced with data protection compliance issues. This can be neatly illustrated by two recent examples. First, on 12th June 2017, the Information Commissioner's Office (ICO), the United Kingdom's (UK) Data Protection Agency, fined Gloucester City Council £100,000 after a cyber attacker was able to gain access to council employees' sensitive personal information. The second high-profile example which, despite not involving any monetary penalty, was arguably more significant, was the DeepMind saga. Specifically, on 3rd July 2017, in a letter to the Royal Free NHS Foundation Trust the ICO articulated a number of concerns it had in respect of the affiliation between the NHS and DeepMind Technologies Ltd, a British artificial intelligence company tasked with undertaking various personal data processing operations on behalf of the NHS. Notably, the ICO stated that *"the processing of*

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, pp. 1–88.

[2] Officially known as Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [hereinafter the DPD]

approximately 1.6 million patients' personal data by DeepMind Technologies Limited ('DeepMind') for the purpose of the clinical safety testing of the Streams application did not fully comply with the requirements of the Data Protection Act 1998."[3]

An observable trend in eGovernment initiatives throughout Europe in recent years has been the emergence and rollout of electronic identity schemes that allow individuals to manage and authenticate their identities in conjunction with the use of online public services. Against this background, the UK Government has recently been developing its own electronic identification (eID) scheme, Gov.UK Verify. This service, which delegates the verification of users' identities to a range of certified private companies, claims to provide a safer, simpler, and faster way of accessing government services.

The development of GOV.UK Verify can also be situated in the context of the encouragement of the deployment of electronic schemes at the European Union level with the adoption of the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS)[4] in 2014, two years prior to the adoption of the GDPR. To be clear, eIDAS does not impose the creation of national eID schemes as such, but aims to ensure their interoperability through the application of the principle of mutual recognition once Member States decide to notify their national schemes to the European Commission.

Importantly, eIDAS makes it clear that the processing of personal data inherent in national eID schemes must comply with EU data protection law.[5] Obviously, in 2014 the EU's leading legislative instrument in the data protection field was the DPD. However, in some ways eIDAS could be described as anticipating the GDPR. For instance, in eIDAS' text one can find express references to key GDPR concepts such as privacy by design.[6] The use of eID schemes as a means of managing identities necessarily involves the processing of individuals' personal data and, consequently, means that all such services, including GOV.UK Verify, must comply with EU data protection law. Importantly, Brexit, i.e. the UK leaving the European Union, should not affect this requirement. The message from the UK government and the ICO has always been that the substance of the GDPR, if not the GDPR itself, will be part of UK law.[7] The strongest commitment to this ideal to date being the recent announcement of a new Data Protection Bill designed to transpose the terms of the GDPR into UK law.[8]

---

[3] Elisabeth Denham, Information Commissioner, Letter to Sir David Solman, 3rd July 2017, available at: https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf.

[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC OJ L 257, 28.8.2014, pp. 73–114.

[5] Article 5(1) eIDAS.

[6] Generally speaking, the term "Privacy by Design" refers to an approach to the construction of technological communications systems, data processing technologies, and computer networks in which privacy is taken into account at all stages of the design process. On this topic, see: Cavoukian, A. (2011) "Privacy by Design", *Information & Privacy Commissioner of Ontario*.

[7] Out-Law.com (last accessed October 2017) "GDPR will come into force in the UK in 2018, minister confirms", https://www.out-law.com/en/articles/2016/november/gdpr-will-come-into-force-in-the-uk-in-2018-minister-confirms/.

[8] Gov.UK (last accessed October 2017) "Government to strengthen UK data protection law", https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law. The Data Protection Bill was introduced to the House of Lords on 13 September 2017, See: Gov. UK (last accessed October 2017) "Data Protection Bill 2017", https://www.gov.uk/government/collections/data-protection-bill-2017.

This article focuses on the issue of data protection law compliance in the context of eID schemes and examines GOV.UK Verify's compliance with some substantive provisions of the EU data protection framework. It identifies some inadequacies inherent in GOV.UK Verify's general setup in the light of the GDPR and ultimately argues that its operation lacks an adequate legal basis. Essentially, the reason for this is because, despite the detailed allocation of roles between the different GOV.UK Verify actors, the process of electronic identification by the identity providers involved creates a situation of joint controllership.

GOV.UK Verify is therefore used as a case study to illustrate one key compliance challenge brought about by the GDPR which is relevant for both private and public entities: the establishment of a proper legal basis for the processing of personal data. Notably, the GDPR provides that "*infringements of [the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9] shall …be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher*."[9] Accordingly, the choosing of an appropriate legal basis for personal data processing is evidently a crucial exercise for legal compliance purposes. Interestingly, in the DeepMind affair, mentioned above, the ICO did not deem it necessary to issue any monetary penalty even though several violations of the UK Data Protection Act were found to have occurred, one of which being the fact that Deep Mind's personal data processing activities had an erroneous legal basis.

The legal assessment of Gov.UK Verify is then pushed further. Having highlighted how establishing an appropriate basis for the processing of personal data is an important and difficult compliance challenge, the article also suggests that if a situation of joint controllership can be established, not only will the dual legal basis identified for the UK eID scheme be problematic, but issues will also arise in conjunction with the liability stipulations found in the framework agreement governing the relationships between the Government Digital Service and certified service providers, i.e. identity providers. Yet, given the inclusion of a right to compensation in the GDPR, based on a presumption of liability the framework agreement is problematic from a legal compliance standpoint. It is true, for instance, that Article 11 of eIDAS itself contains a provision on liability. However, it is argued that to make Article 11 of eIDAS compatible with Article 82 of the GDPR, GDPR Article 82 should be applied if the damage caused to a natural or legal person is the result of an infringement of the GDPR, e.g. security obligations as per Article 32 GDPR, as eIDAS legislative intent is neither to derogate from EU data protection law nor to set lower standards of data protection,

To this end, the article consists of four main sections. The first section comprehensively outlines GOV.UK Verify, drawing attention to its technical and operational dimensions, including the substance of the data protection impact assessment (DPIA) performed during its design stages. The second section sketches and discusses the various legal bases for the processing of personal data as enshrined within the EU data protection framework. The third section suggests that the processing of personal data by identity providers should be considered a situation of joint controllership and thereby adds an element of complexity to the picture by analysing the implications of such a characterisation for establishing an adequate legal basis for personal data processing. It thus provides insight as to how the concept of joint controllership should be interpreted in practice, which should have relevance for

[9] Article 83(5) General Data Protection Regulation.

other cases such as the DeepMind saga.[10] The final substantive section then derives the consequences of the characterisation of a situation of joint controllership for the allocation of liability between the different stakeholders, and raises a fundamental question for the consistency of the legal framework built for sustaining the EU digital single market: how can eIDAS and the GDPR be combined? Notably, this high-level question is not a one-shot interrogation and similar questions arise in conjunction with other pieces of legislation, such as the proposal for a new ePrivacy Regulation released in January 2017.[11]

The ambition of this article is, therefore, to highlight the limits of a regulatory approach implemented in silos. The article is a product of a desk research methodology, which was contextual and interdisciplinary in nature, and targeted traditional primary and secondary legal sources but also soft law instruments such as data protection agencies' guidance, design and contractual documents such as data protection impact assessments or framework agreements and focusing upon a specific scenario of electronic identification. It ultimately suggests that the traditional interpretative principle of *"lex specialis derogat legi generali,"* is not suitably geared towards solving conflicts arising between the GDPR and eIDAS. This is despite the fact that this approach has previously been used on occasion by the Court of Justice of the European Union (CJEU) to solve conflicts between different pieces of legislation.

2. GOV.UK Verify: a case study

To perform a legal assessment of GOV.UK Verify it is first necessary to reflect upon the inception of the project, outline its architectures, identify its main actors, map the data flows between the different components of the system, and consider the perceptions of those involved in the design of the scheme in relation to the data protection implications and challenges inherent in its establishment.

2.1 The History

In 2013 the UK Government published its 'Government Digital Strategy'. One of the strategy's central points was to transition all public services to a 'Digital by Default' operation, whereby electronic transactions would be the default means of transacting with members of the public.[12] Action 11 of the Government's transformation plan promised that the Government Digital Service (GDS) would "*develop a framework to enable federated identity assurance to be adopted across government services in due course*."[13] Identity assurance emerged as a response to the previous failed attempt to introduce an identity card for all citizens, a proposal which would have required the establishment of a central 'National Identity Register' and an electronic identification functionality.[14] The proposal for a National Identity Register was met with concern, and the plan for identity cards and the central

[10] It is however striking to note that the ICO decided to assess Deep Mind's practices on the basis that Deep Mind was only a processor and not a data controller. See: ICO (last accessed August 2017) "Royal Free - Google DeepMind trial failed to comply with data protection law", https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

[11] Proposal for a regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final.

[12] Cabinet Office (last accessed October 2017) "Government Digital Strategy: December 2013" https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy - "*Digital by default means digital services which are so straightforward and convenient that all those who can use digital services will choose to do so, while those who can't are not excluded*."

[13] *Ibid* Action 11.

[14] Identity Cards Act 2006 c 15 s1.

Register were scrapped with the enactment of the Identity Documents Act 2010.[15] Subsequent plans for electronic identification focused on software tokens and de-centralised approaches.

The GDS' `Identity Assurance Programme', later named 'GOV.UK Verify', was developed to replace the 'Government Gateway' platform, which was used to access most public services.[16] In the UK Digital Strategy for 2017, GOV.UK Verify is described as "*a federated, market-based approach to identity assurance for central government that can be reused in the wider public and private sectors.*"[17] It has been designed around a set of "*Identity and Privacy Principles*",[18] focused on "*individual control and* consent".[19] The principles were set up by an advisory group, whose purpose is to safeguard users' privacy.[20] Amongst them, Principle 1 prescribes that the user "*can exercise control over identity assurance activities*" which "*can only take place if [they] consent or approve them*"[21] and Principle 4 concerning Data Minimisation mandates that "*interactions only use the minimum data necessary*".[22]

2.2 Architecture and actors

The premise behind GOV.UK Verify's design is the notion that eID schemes should not operate under the sole control of a central Governmental agency. The 9 "*Identity and Privacy Principles*"[23] specify minimum standards in respect of any eID scheme's operation. The principles aim at a technology-neutral approach; they form targets the system should achieve but do not dictate specific means as to how to achieve them. GOV.UK Verify focuses heavily on user choice: specifically, the idea that the user should be able to decide the number of eIDs they own, as well who is able to access and hold their personal data.[24] Hence the creation of an 'Identity marketplace' was settled upon. Although the marketplace is based on a public platform, a hub which is owned and controlled by the GDS, the electronic identification of users is provided by private companies who act as Identity Providers.

Identity Providers have to be certified "*against common governance requirements*", under the Identity Assurance Principle no. 7.[25] Certification, as outlined in the Framework agreement,[26] is three-fold: (a)

[15] 2010 c 40 ss. 1-3.
[16] Government Gateway (last accessed October 2017) 'What is the Government Gateway', available at: http://www.gateway.gov.uk/Help/Help.aspx?content=help_more_info_gateway.htm
[17] Cabinet Office (2017) "UK Digital Strategy 2017" https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy" ch 6.
[18] Privacy and Consumer Advisory Group (2014) *Identity Assurance Principles*, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf> [preserved at: https://perma.cc/5K2W-8BVK]
[19] *Ibid* p. 3.
[20] Cabinet Office (2014) "Privacy and Consumer Advisory Group", available at: https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group. "*PCAG aims to ensure: users are in control of their information[;] information isn't centralised[;] users have a choice of who provides services on their behalf*".
[21] *Ibid*.
[22] *Ibid*.
[23] (1) The User Control Principle; (2) the Transparency Principle; (3) the Multiplicity Principle; (4) the Data Minimisation Principle; (5) the Data Quality Principle; (6) the Service-User Access and Portability Principle; (7) the Governance/Certification Principle; (8) the Problem Resolution Principle; (9) the Exceptional Circumstances Principle. *See Privacy and Consumer Advisory Group, Identity Assurance Principles, n. 18.*
[24] *Ibid*, the Multiplicity Principle: "*I can use and choose as many different identifiers or identity providers as I want to*."
[25] *Principles* n. 18 pg.10.
[26] Cabinet Office, (2014) "Framework Agreement and Schedules" Draft v0.9, pg.18. available at:http://data.gov.uk/data/contracts-finder-archive/contract/1690273/

certification against industry standards for information security,[27] certification that they meet government standards for identity assurance,[28] and complies with data protection law (certified through a Privacy Impact Assessment).[29] In relation to certification for identity assurance, the Framework explicitly mentions tScheme as the certification body.[30] tScheme is the "*Trusted List Scheme Operator (TLSO) and creates, hosts and maintains the UK's Trust Service-status List (TSL) on behalf of the Department for Business, Energy and Industrial Strategy (BEIS)*"[31] of the Qualified Trust Service Providers required by eIDAS.[32] It accredits certification to Identity Providers against five 'Approval Profiles'.[33] It is not clear, however, how many of these profiles an Identity Provider necessarily needs to satisfy to become certified. However, it is worth noting that several of the current certified providers have been accredited with four or five of these profiles.[34] It is also interesting to note that not all providers in GOV.UK Verify's list are certified (particularly, the Post Office is one notable example of a provider that has not been certified by tScheme)[35] and that communication from the GDS considers evidence of "*working towards independent certification*" to be an acceptable criterion for becoming a provider.[36] Electronic identification is organised according to 'Levels of Assurance' (LOA), a risk-based assessment based on the "*degree of confidence the government service requires that a user is who they say they are*."[37] The system uses software credentials for identification, a combination of "*usernames, passwords and security codes*."[38] Communication within the GOV.UK Verify federation happens through the Security Assertion Markup Language (SAML 2.0)[39] and data are signed and verified through a Public Key Infrastructure (PKI).[40]

---

[27] The Framework mentions ISO 27001 and ISO 15489-1, but accepts other equivalent standards: ibid, s. 8.10(g) and sch. 5(a)(2)(b).

[28] *Ibid* s. 8.10(f)j and sch. 5(a)(2)(a)(i).

[29] *Ibid*, sch. 5(a)(2)(d).

[30] *Ibid*, pg. 83, although the government retains the right to change the certification body in the future: "any organisation that has been approved for the assessment of trust services to the satisfaction of the Authority and that has been notified by the Authority as a Certification Body from time to time".

[31] Energy and Industrial Strategy Department for Business (2016) *Electronic Signatures and Trust Services*, pg.9. available at:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/beis-16-15-electronic-signatures-guidance.pdf

[32] tScheme, (last accessed October 2017) 'UK's Trusted List' (*Support for the eIDAS Regulation*, 2017) http://www.tscheme.org/UK_TSL/index.html

[33] Base Approval Profile (tSd0111); Profile for Identity Registration (tSd0108); Profile for Credential Validation (tSd0109); Profile for Attribute Registration (tSd0110); Profile for an Identity Provider (tSd0112); Profile for Credential Management (tSd0113): tScheme (last accessed October 2017) "Digests of Approval Profiles for IdP-related Services" http://www.tscheme.org/profiles/IdP_digest_2.html.

[34] See for example Experian's Grant of Approval who satisfies four (http://www.tscheme.org/directory/EXPN_IDaaS/index.html) compared to Barclays' which satisfies five (http://www.tscheme.org/directory/Barclays/index.html).

[35] GDS justifies this omission by explaining that the Post Office uses the system of another provider to offer its services and therefore the certification of the other provider is deemed enough. See: Gov.uk (last accessed October 2017) "Working with identity providers as they become certified companies", https://identityassurance.blog.gov.uk/2015/12/03/working-with-identity-providers-as-they-become-certified-companies/#comment-41610.

[36] Alastair Williamson-Pound, A. Gov.UK Verify Blog (2016) (last accessed October 2017) "Becoming a GOV.UK Verify certified company", https://identityassurance.blog.gov.uk/2016/02/25/becoming-a-gov-uk-verify-certified-company

[37] Government Digital Service (2014) 'Gov.UK Verify Technical Guide', Glossary of terms, available at: http://alphagov.github.io/rp-onboarding-tech-docs/index.html

[38] *Ibid*.

[39] Cabinet Office, *Identity Assurance Hub Service SAML 2.0 Profile v1.2a*, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/279643/Identity_Assurance_Hub_Service_Profile_v1.2a.pdf

[40] Identity Assurance Team (2015) *Identity Assurance Documentation*, available at: https://media.readthedocs.org/pdf/random/latest/random.pdf

Levels of Assurance (LOA)

LOA 1	Used when a government service needs to know that it's the same user returning to the service but doesn't need to know who that user is.
LOA 2	Used when a government service needs to know on the balance of probabilities who the user is and that that they are a real person.
LOA 3	Used when a government service needs to know beyond reasonable doubt who the user is and that that they are a real person.
LOA 4	As level of assurance 3, but with a biometric profile captured at the point of registration.

Table 1: the four different LOA[41]

Gov.UK Verify's architecture thus comprises five key elements:

(1) The **Federation Hub**: a central infrastructure that mediates all interactions between users, Identity Providers and Services (or Service Providers). The Hub leases eID services from the private Identity Providers. The Hub acts as a broker to exchanges between parties. These exchanges which are concealed from the different parties, ensuring that the Identity Provider itself remains unknown to the Service Provider. The Hub ensures that the required LOA is adhered to and does not collect or store data beyond the current session (stateless operation).[42]

(2) The **Service Provider**: Service providers are the different public services that can request the electronic identification of the user in order to transact with them. At the moment, service providers in the GOV.UK Verify federation are solely governmental departments.[43]

(3) The **Identity Provider**: Identity providers are "[p]*rivate sector organisations, paid by the government, to verify that a user is who they say they are and assert verified data that*

[41] Government Digital Service, 'Gov.UK Verify Technical Guide' (n. **Error! Bookmark not defined.**), Glossary of terms; Cabinet Office (2014) 'Good Practice Guide No. 45: Identity Proofing and Verification of an Individual', pg.9. available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf
[42] *Ibid*, Architecture.
[43] *Ibid*, Glossary 'Relying party'.

identifies them to a government service."[44] They verify the user's identity against various authoritative sources, like the HM Passports Office and the Driving Licensing Authority (DVLA).[45]

(4) The **Matching Service**: a middleware deployed at the Service Provider level the purpose of which is to match the eID received by the Identity Provider to a local account in the Service Provider's database.

(5) The **Document Checking Service**: a supplementary service designed and operated by the Government Digital Service (GDS), whose role is to check the official documents provided by the user against authoritative sources. At the moment, checks are performed against the HM Passport Office or the DVLA.[46] The system returns an attestation of the authenticity of the documents to the Identity Provider, meaning that Identity Providers are not required to directly access official records. The Document Checking Service is not engaged in every eID transaction; instead it is only needed for the registration of a new user with an Identity Provider

From this description, it thus appears that the Gov.UK Verify system involve 4 actors:

1. The **GDS**, operating the Federation Hub and the Document Checking Service.
2. Government Services acting as relying parties, which request authentication (in the sense of verification of identity) and which host matching services also characterised as **service providers**.
3. Certification companies acting as **identity providers**.
4. **Service users**.

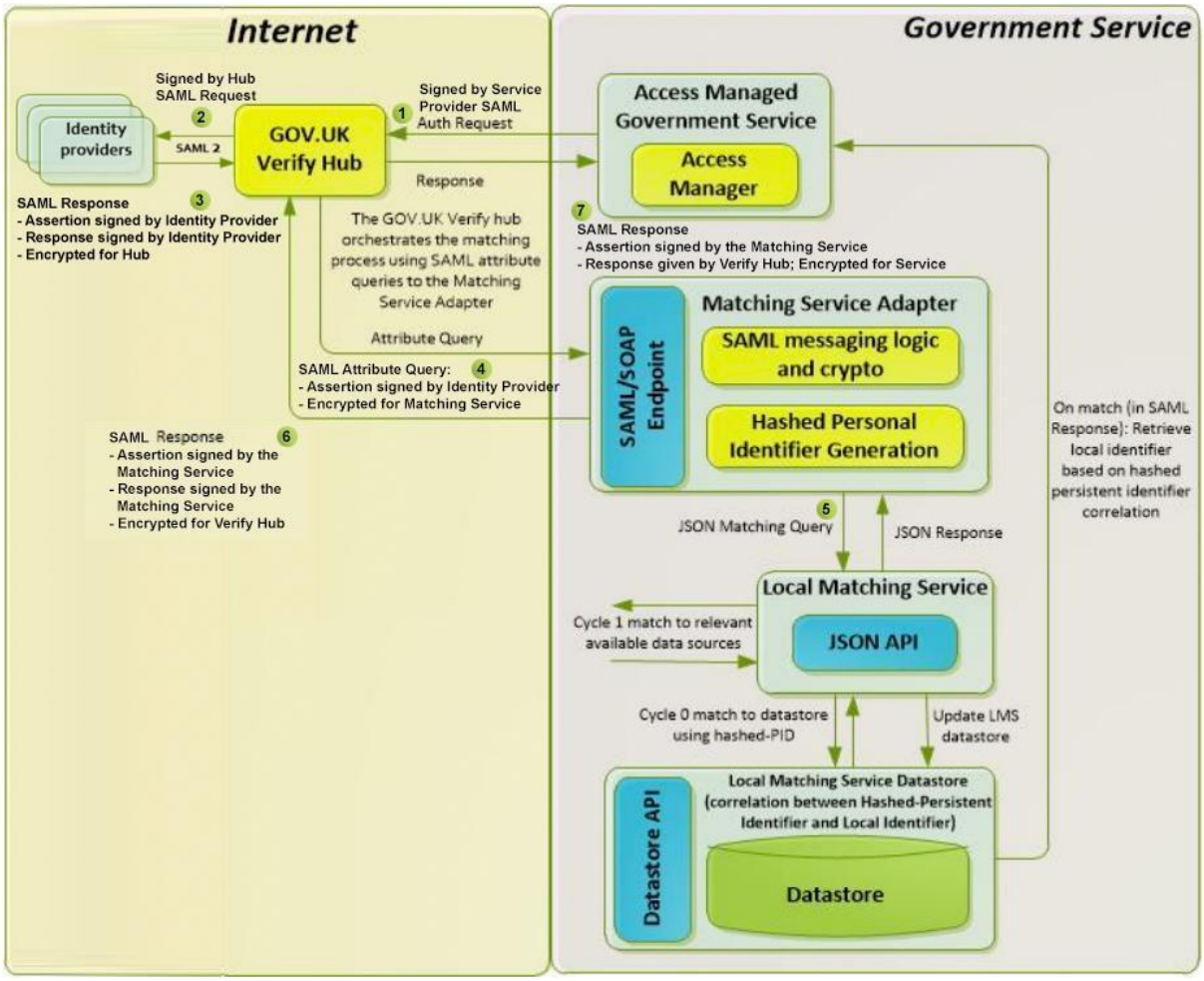

Figure 1: Gov.UK Verify actors and data flows (adapted)[47]

2.3 Data flows

The typical user journey in Gov.UK Verify starts when a user requests an identification against a governmental service. The service sends an authentication request to the Hub (step 1, Figure 1) indicating the requested LOA (at the moment Gov.UK Verify supports only LOA 2).[48] The request is signed by the Service Provider. The Hub prompts the user to select one of the available Identity The typical user journey in GOV.UK Verify starts when a user asserts their identity when attempting to access a governmental service. The service sends an authentication request to the Hub (step 1, Figure 1) indicating the requested LOA (at present GOV.UK Verify supports only LOA 2).[49] The request is signed by the Service Provider. The Hub prompts the user to select one of the available Identity Providers, depending on the available data the user has made available for the purposes of verifying their identity. An authentication request is sent to the selected Identity Provider, signed by the Hub (step 2, Figure 1). The Identity Provider verifies the user's identity according to the indicated LOA. The verified identity (the eID) is sent as a response to the Hub, signed by the Identity Provider (step 3, Figure 1). The eID contains an 'authentication assertion' – encrypted for the Hub – which asserts that the user's identity is authenticated and contains contextual information including the LOA.[50] It also contains an 'Identity assertion', also encrypted for the Hub, containing two elements: the Matching Dataset and a Persistent Identifier. The Matching Dataset comprises of the same information for every eID.[51] The Persistent Identifier is a pseudo-random value generated by the Identity Provider and refers to the combination of the user and the chosen identity provider.[52] The 'Identity assertion' is then sent by the Hub to the Matching Service located at the Service Provider. The 'Identity assertion' retains the signature of the Identity Provider and is encrypted for the Matching Service (step 4, Figure 1). The Matching Service then performs a series of attempts to match the 'Identity assertion' to a local user record, a process known as 'matching cycles'. The first cycle, 'cycle 0', starts when the Matching Service changes the Persistent Identifier to a hashed value, which is created by a combination of user, Identity Provider and Service Provider.[53] After the creation of the hashed persistent identifier, the Matching Service looks up a local datastore to see if the same hashed value already exists and whether it can be associated with a local record. If a match is found, the 'Identity assertion' along with the hashed identifier are forwarded to the Service Provider. If not, the Matching Service tries to determine a match using the values of the matching dataset ('cycle 1'). If no match is found subsequent cycles will ask the user for additional attributes. When a match is found the Matching Service sends a 'match' response along with the 'Identity assertion' back to the Hub, signed by the Matching Service and encrypted for the Hub (step 6, Figure 1). The Hub sends the signed 'Identity assertion' in an encrypted form to the Service Provider (step 7, Figure 1), which then retrieves the local record from its database.

[47] Identity Assurance Team, *Identity Assurance Documentation* (n. **Error! Bookmark not defined.**), pp. 7-9.
[48] Government Digital Service, 'Gov.UK Verify Technical Guide' (n. **Error! Bookmark not defined.**), 'Architecture'.
[49] Government Digital Service (2014) 'Gov.UK Verify Technical Guide' n. 26, 'Architecture'.
[50] *Ibid*, 'How SAML works with Gov.UK Verify'.
[51] *Ibid*, Glossary 'Matching dataset'.
[52] *Ibid*, Glossary 'Persistent identifier (PID)'.
[53] *Ibid*, Glossary 'Hashed persistent identifier (PID)': "This ensures that identifiers for user identity are unique to specific services and can't be used across multiple services."

Matching Dataset
First name
Middle name (if provided)
Surname
Address
Date of birth
Gender (optional)

Table 2: Gov.UK Verify's Matching Dataset

2.4 Gov.UK Verify Data Protection Impact Assessment

While GOV.UK Verify's data protection impact Assessment (DPIA) was obviously undertaken before 25th May 2018, the date at which the GDPR becomes applicable, it was published on 18th May 2016, after the public release of the final text of the GDPR, which, as noted above, was adopted on 25th May 2016.[54] The authors of the DPIA were, therefore, fully aware of the content of the GDPR at the time of the impact assessment's release. This is well evidence by the way in which the title of the impact assessment document was altered in order *"to reflect the terminology of the new EU General Data Protection Regulation."*[55] Despite demonstrating an initial general awareness of the GDPR, however, the drafters of the DPIA recognised that a second impact assessment would be required at a later date in order to fully take into account the changes brought about by the GDPR. It is therefore expressly stated in the document that the *"DPIA does not consider the requirements of the EU General Data Protection Regulation (GDPR), since the final text was only approved in May 2016."*[56] However, more than one year after the publication of the initial DPIA no new impact assessment has been released to the public.

[54] The first version of the data protection impact assessment is dated 27 January 2015. The document was then modified on 15 February 2015, 31 March 2016, and several times in May 2016 (13 May 2016, 16 May 2016 and 18 May 2016). An initial data protection impact assessment had been conducted in September 2014 for project approval purposes.
[55] DPIA, pg. 6.
[56] *Ibid*, pg. 7.

The DPIA is said to follow the approach advocated by the ICO in its code of practice on data protection impact assessment but with a notable caveat. Particularly, it:

> *"...has been modified to take into account other specific requirements for the GOV.UK Verify environment, most notably the Identity Assurance Principles published by the Cabinet Office Privacy and Consumer Advisory Group (PCAG)."*[57]

The approach has been described as being aligned to the requirements of ISO2001 standards.[58] The DPIA identifies three data controllers: the GDS, the Certified Companies and Government Services.[59] We therefore have at least two public authorities and a set of private actors acting as data controllers for the purposes of data protection law. In regards to identifying the legal basis for the processing of personal data in this context, two prominent possibilities appear to emerge: the individuals' whose personal data are involved giving their consent, and justifying the processing of personal data on the basis that said processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller:

> *"GOV.UK Verify uses consent to enable processing, and processing is also enabled by Data Protection Act Schedule 2 Part 5 (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government, and (d) for the exercise of any other functions of a public nature exercised in the public interest by any person."*[60]

Having said this, consent as a legal basis seems to be used for one type of processing and thereby one type of relationship: the processing undertaken by certified companies at the request of service users. One can read to that effect:

> *The Certified Company obtains consent to operate an account for the Service User, and to collect, share and maintain the personal information in order to verify and maintain the servicer user's identity. The Certified Company obtains consent from the Service User to release matching data to the Federation Hub and on to the Government Service, at the request of the Service User.*[61]

The importance of consent in the relationship between service users and certified companies is also described as being the result of the implementation of the first identity assurance principle. As noted above, the identity assurance principles are principles that have been developed to support the creation of an identity assurance service. The first identity assurance principle is formulated in these terms:

> *"I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them."*[62]

---

[57] *Ibid*, pg. 6.
[58] *Ibid*, pg. 7.
[59] *Ibid*, pg. 10. See also Table 2: stakeholder analysis pg. 17.
[60] *Ibid*, p. 10.
[61] *Ibid*
[62] Privacy and consumer advisory group (PCAG), Identity Assurance Principles, version 3.1, pg. 8, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf

However, consent does not seem to be of use solely to certified companies. To the question as to whether *"suppliers/partners have the right to use the personal information collected or shared under the service for their own purposes"*[63] the answer appears to be that *"Government Services may use information for their own purposes, but will have to disclose purposes and details of information required to the service user on a per-transaction basis, and seek appropriate consent."*[64]

Interestingly, GOV.UK Verify's DPIA does not adhere to the terminology of eIDAS. eIDAS distinguishes between three types of actors for the operation of eID schemes: the notifying Member State, the party issuing the electronic identification means, and the party operating the authentication procedure. The electronic identification means is defined as per Article 3(2) eIDAS as:

> *"a material and/or immaterial unit containing person identification data and which is used for authentication for an online service."*

In the context of GOV.UK Verify identity providers are thus the parties issuing the electronic means of identification, even if a matching service sits within each (government) service provider. In respect of the party operating the authentication procedure, however, the characterisation may be less straightforward. Article 3(5) eIDAS defines authentication as:

> *"…an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed"*

In the context of GOV.UK Verify, the GDS should be characterised as the party operating the authentication procedure, to the exclusion of (Government) service providers. The combination of Articles 11(3) and 7(f) eIDAS is however not obvious as although Article 11(3) targets the party operating the authentication procedure and refers back to Article 7(f), Article 7(f) itself only mentions the notifying Member State.

From this introduction to the conception of the UK eID scheme, it appears that consent was, and presumably still is, intended to play a prominent role in legitimising the processing of personal data for purposes of user authentication. Concurrently, it is important to note that consent has never been, nor should it be, thought of as the exclusive legal basis through which the processing of personal data can be legitimised. Still, in order to provide a platform from which the choices made by the GDS can be assessed, as the GDPR does not exactly repeat the same words as the DPD, it is worth verifying what the implications of the GDPR are, or at least should be (as obviously the GDPR has not been litigated yet and therefore interpretation can only be tentative), in respect of choosing an appropriate legal basis for personal data processing.

3. Choosing the appropriate legal basis

The requirement of lawfulness of personal data processing spans a relatively large range of legal bases. Only those that appear to be the most relevant for the activities of electronic identification within the framework of an eID scheme will be examined in this section: individual consent, processing that is necessary for the conclusion or performance of a contract to which the data subject is a party, processing that is necessary for the performance of task carried out in the public interest or in the exercise of official authority vested in the controller, and processing that is necessary for the

63
64

purposes of the legitimate interests of the data controller or other third party. The dual legal basis relied upon by GOV.Uk Verify is then assessed in the light of a consideration of these abovementioned examinations. This exercise necessarily requires going back to the DPD to determine whether, how, and to what extent, the GDPR goes beyond it.

3.1 The legal bases for personal data processing and their applicability to GOV.UK Verify

As alluded to above, the European data protection law imposes a range of substantive requirements on any act of data processing that involves personal data. Personal data is an expansive concept, which encompasses any information that can be related to an identified or identifiable information, and thus includes, but is not limited to, an individual's name, age, race, gender, sexual preferences, political affiliations, internet search histories, and health and financial information.[65] Processing is a similarly broad term, which is taken to encompass almost any form of personal data usage.[66]

Perhaps the most significant substantive requirement imposed by the European data protection framework is the fact that the processing of personal data will only be considered lawful if one, or more, of a finite number of prescribed legitimising grounds for that processing can be identified. Namely, in order for the processing of personal data to be rendered lawful the controller of those data must show that either: the individual to whom those personal data relate has given their consent to their personal data being processed for a specific purpose; the processing is necessary for the performance of a contract; the processing is necessary for compliance with a legal obligation to which the data controller is subject; the processing is necessary in order to protect the vital interests of the data subject or another natural person; the processing is necessary for the performance of a task carried out in the public interest; or the processing is necessary for the purposes of the legitimate interests pursued by the data controller or another third party.[67]

For several reasons, it would appear that GOV.UK Verify must comply with data protection law's substantive provisions. Firstly, as has been noted elsewhere, all data processing activities involving individuals' personal data that are undertaken by either private or public-sector bodies fall within the scope of data protection law unless they have been specifically omitted. A notable of such an omission being data processing activities that are undertaken in conjunction with law enforcement proceedings.[68]

At this point it is important to recall that GOV.UK Verify has a somewhat unusual structure in that it cannot accurately be described as a completely private or public-sector service. Instead, GOV.UK Verify might best be described as a Public-Private Partnership, a term broadly used to refer to

[65] See: Article 2(a) Data Protection Directive and Article 4(1) General Data Protection Regulation.
[66] See: Article 2(b) Data Protection Directive and Article 4(2) General Data Protection Regulation; Case C-101/01 Bodil Lindqvist, EU:C:2003:596; Case C-461/10 Bonnier Audi AB and others v Perfect Communication Sweden, EU:C:2012:219; Case C-291/12 Michael Schwarz v Stadt Bochum, EU:C:2013:670.
[67] Article 7 Data Protection Directive and Article 6 General Data Protection Regulation.
[68] Purtova, N. (2017) "Between GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships", available at: https://ssrn.com/abstract=2930078; Klingenberg, A. (2016) "Catches to the right to be forgotten, looking from an administrative law perspective to data processing by public authorities", *International Review of Law Computers and Technology*. See also: Article 29 Data Protection Working Party (2013) Opinion 06/2013 on open data and public sector information ('PSI') reuse WP207; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89.

arrangements between government and private sector institutions in which partially or traditionally public activities are performed by private sector organisations.[69] Significantly in this regard, however, as has been argued elsewhere, arrangements which involve private parties entering systematic collaborative endeavours with governmental and other public sector bodies will be subject to the same remit of data protection obligations as any other private or public party.[70]

Secondly, as touched upon previously, the abovementioned eIDAS Regulation[71] defines an interoperability framework of national eID services which requires all Member States to notify the European Commission of the interoperability of their national eID scheme, and demonstrate it conforms to a number of other substantive requirements, if they wish to operate their scheme on a cross-border basis.[72] Successful notification comes after a lengthy deliberation process where Member States make (non-binding) suggestions on the eID scheme in question.[73] Upon acceptance of the notified scheme, all other Member States are obliged to incorporate it into their individual authentication services.[74] Significantly, one notable requirement imposed by the eIDAS Regulation is that in order to achieve successful notification any national eID scheme must comply with the substantive provisions of European data protection law, with specific reference being made to the need to comply with the data minimisation principle.[75] Though the UK government has not signalled its intention to notify GOV.UK Verify, this will surely be required if the scheme is to have any prospect of international success.

The above considerations indicate that Gov.UK Verify must comply with the substantive provisions of European data protection law, including the need for it to have a legitimate basis at all times for the processing of any personal data. In this respect, and as also touched upon above, whilst the data protection framework contains a number of grounds upon which the processing of personal data can be rendered legitimate, in the GOV.UK Verify context two legal bases have been put forward: consent of the individual and performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.[76]

Consent is expressly referred to by the GOV.UK Verify website itself, which specifically states that no personal data will be processed as part of the GOV.UK Verify scheme without the consent of any individuals involved.[77] However, as suggested at this article's outset, there are reasons to believe that GOV.UK Verify does not comply with the European data protection framework's rules regarding consent as a legitimising ground for the processing of personal data. Before examining this notion in more detail, it is first important to consider the doctrine of individual consent under both the DPD and the GDPR, as well as the other legitimising grounds for processing listed by both instruments.

---

[69] Savas, E. (2000) *Privatisation and Public-Private Partnerships*, New York: Chatham House, pg.4. See also: Recital 97 General Data Protection Regulation.
[70] Purtova, N. (2017) Op Cit; Klingenberg, (2016) Op Cit.
[71] Officially known as Regulation (EU) No.910/2014 of 23 July on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.
[72] *Ibid*., Articles 7 and 9.
[73] Tsakalakis, N. O'Hara, K and Stalla-Bourdillon, S. (2016) "Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation", *Proceedings of the 8th ACM Conference on Web Science*, pp.55-65.
[74] Article 6 eIDAS Regulation.
[75] Recital 11 and Article 12 eIDAS Regulation.
[76] n.73 pg.61.
[77] GOV.UK Verify (last accessed October 2017) "GOV.UK Verify: privacy and consent", https://identityassurance.blog.gov.uk/2015/07/30/gov-uk-verify-privacy-and-consent/

3.2 Consent

The consent of the individual is listed as a legitimising ground for the processing of personal data under both the DPD and GDPR. However, the formulations of consent differ between these two legislative instruments, and so it is important to consider them individually in turn.

3.2.1 The Data Protection Directive

Article 2(h) of the DPD defines consent as:

> "*…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*".

Article 7(a) then states that data may be processed when:

> "*the data subject has unambiguously given his consent*".

Accordingly, the giving of free, specific, informed and unambiguous consent is one way by which the processing of personal data can be rendered legitimate under the DPD.[78] In some ways the DPD's definition of consent could be considered somewhat restrictive, as it requires that the individual be clearly informed of what it is they are consenting to in advance of any consent being given. This approach is broadly in line with the existing data protection laws of most EU Member States, many of which have defined consent with similar restrictiveness.[79]

Conspicuously, the DPD's definition of consent is not phrased in terms of whether consent must be "opt-in" (i.e. based on an affirmative act, such as clicking a box on an online form or providing a signature) or "opt-out" (e.g. not unclicking a pre-ticked box). Instead, debates have tended to focus on whether the absence of the term "explicit" suggests that opt-in consent is not required as a general matter.[80]

In this respect, it has thus been suggested that the DPD's definition is somewhat cryptic as well as restrictive, as the use of ambiguous terms like "specific", "freely given" and "informed" allow for a broad spectrum of interpretation.[81] Moreover, the DPD says nothing in respect of the methods data controllers may, or should, use as a means of obtaining consent. However, Article 2(h)'s requirement

[78] Explicit consent, a term which is not defined by the Directive, is required for the processing of data relating to the racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, or the health or sex life of the data subject. Article 8(2)(a) Data Protection Directive.

[79] Kuner, C. (2007) *European Data Protection Law: Corporate Compliance and Regulation*, Oxford: Oxford University Press, pg.67.

[80] The Article 29 Working Party has suggested, however, that in certain situations an opt-in approach may be required. In an "Opinion on unsolicited communications for marketing purposes it stated that "*Implied consent to receive such mails is not compatible with the requirement of consent being the indication of someone's wishes, including where this would be done 'unless opposition is made'…Similarly, pre-ticked boxes, e.g., on websites are not compatible with the definition of the Directive either"*. See: Article 29 Working Party (2004) Opinion 05/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC WP90. Nevertheless, in certain jurisdictions, notably the United Kingdom, opt-out approaches to consent have previously on occasion been considered acceptable. See *Linguaphone Institute v Data Protection Registrar* Case DA/94 31/49/1.

[81] Kosta, E. (2013) *Consent in European Data Protection Law*, Boston: Martinus Nijhoff Publishers, pg.109.

that the data subject must "signify" their consent implies that complete inaction on behalf of the individual will not be sufficient to amount to valid consent.[82]

The Data Protection Act 1998 (DPA) is currently the UK's most significant legislative instrument in the data protection field and transposes the terms of the DPD into the UK's domestic legal order. In accordance with what is said in the DPD, Schedule 2 of the DPA states that for the processing of personal data to be rendered lawful said processing must fall under one of the abovementioned legitimising grounds for processing, one of which is the consent of the individual. The DPA, however, contains no definition of consent, nor any guidance as to what is required to validly obtain it.

In lieu of any concrete guidance in respect of consent's interpretation being offered by the texts of the DPD and DPA themselves, the Information Commissioner's Office,[83] the UK's independent regulatory body responsible for matters regarding privacy and data protection, has offered its own views on how consent should be understood. Notably, in its 2017 guide to data protection, the ICO agrees that the DPD's inclusion of the word "signify" means that an individual's consent must be actively communicated if it is to be considered valid, and that valid consent cannot be inferred from a failure to communicate. It is also expressly stated that any consent obtained by way of duress or misrepresentations will not adequately satisfy the conditions for the processing of personal data.[84] The ICO also advises that an individual's consent should be "*absolutely clear*", and that it must at the very least cover the types of information to be processed, the purposes of any processing, and any special aspects of that processing that may affect the individuals whose personal data are involved.[85]

Additional guidance as to the interpretation of consent can also be found in UK case law. In *British Gas Trading v Data Protection Registrar*,[86] for instance, the British Data Protection Tribunal drew a distinction between new and existing customers of British Gas to determine when data protection law's consent requirement would be satisfied. The Tribunal held that new customers of the company would be taken to have consented to their personal data being used for advertising purposes if they had the option to opt-out in the initial contract for service. In respect of already existing customers, however, it was held that a failure to return an opt-out form would not amount to true consent.[87] Beyond providing enough information to the individual in order for them to express consent, in order for an individual's consent to be considered validly obtained the individual from whom the consent is sought must also be afforded a reasonable opportunity to express their consent, or the lack thereof.[88]

Outside of the field of data protection law, other UK cases have also provided some general guidance on the meaning of consent in other contexts, many of which correlate strongly with the abovementioned ICO guidance and data protection cases. As a general matter, it would appear, for instance, that in both criminal and civil law contexts for an individual's consent to be considered valid the consenting individual must have been made fully aware of what it is to which they are giving their

[82] n.79 pg.68.
[83] [hereinafter ICO]
[84] ICO (2017) The Guide to Data Protection, pg.102. Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-7.pdf
[85] *Ibid*
[86] *British Gas Trading Ltd v Data Protection Registrar* [1998] 1 Info. T.L.R. 393.
[87] The judgment in this case seemingly echoed the Tribunal's earlier decision in *Linguaphone Institute v Data Protection Registrar*. Case DA/94 31/49/1.
[88] *Innovations (Mail Order) Ltd v Data Protection Registrar* Case DA/92 31/49/1.

consent,[89] and that valid consent cannot be obtained by way of duress nor expressed through entirely passive acquiescence.[90]

The Article 29 Working Party has also on occasion given its advice on consent's true meaning and how it should be understood in the data protection context. Notably, in its 2011 opinion on the definition of consent, the Working Party examined the concept very closely, specifying several key criteria that must be met for an individual's consent to be considered valid.[91] Notably, the Working Party concluded that only statements or actions that unambiguously indicated an individual's agreement would constitute valid consent. Whilst this did not specify whether consents must be "opt in" or "opt out", the clear implication was that the complete inaction of the individual would never be enough to amount to genuine consent.[92] Furthermore, it was made clear that for consent to be considered freely given, and therefore valid, notice must be provided to the individual in clear and understandable language prior to any processing of personal data occurring, and that in the event of an individual withdrawing their consent the data controller must delete any personal data pertaining to that individual unless another legal basis that justified the storing of those data could be identified.[93]

3.2.2 The General Data Protection Regulation

As explained above, the General Data Protection Regulation[94] has been drafted as a means of bringing the European data protection framework into alignment with contemporary data-handling practices and will be directly applicable and binding in full on all EU Member States from May 2018. Despite "Brexit", and the UK setting a course to leave the EU, the UK Government has confirmed it still intends to implement the substantive terms of the GDPR.[95]

The upshot of this is that to from May 2018 at the latest the DPA will no longer apply and, to all intents and purposes, will effectively be replaced in its entirety by the GDPR and complementary national legislation. Significantly, for the purposes of this article, the GDPR retains the consent of the individual as a legitimising ground for the processing of personal data,[96] but contains a revised, and apparently narrower, definition of consent, which differs from its DPD equivalent. Specifically, the GDPR defines consent as:

> "*…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"[97]

[89] See, for example: *Re Caughey ex p. Ford* (1876) 1Ch.D.521; *A-G's Reference (No 6 of 1980)* [1981] 2 All ER 1057; *R v Barnes* [2004] EWCA Crim 3246.
[90] See: *Bell v Alfred Franks and Bartlett Co Ltd* [1980] 1 ALL ER 356.
[91] Article 29 Data Protection Working Party (2011) Opinion 15/2011 on the definition of consent, WP 187.
[92] This finding echoed an earlier judgment of the CJEU in the *Bavarian Lager* case, where it was held that silence, or a failure to respond, could never form the basis of "free and informed" consent. See: Case C-28/08 European Commission v Bavarian Lager Co, EU:C:2010:378.
[93] Article 29 Data Protection Working Party (2011) Op Cit. See also: Article 7 Data Protection Directive.
[94] Officially known as Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 [hereinafter GDPR]
[95] Supra, n.7.
[96] See: Recital 40 and Article 6(1) General Data Protection Regulation.
[97] Article 4(11) General Data Protection Regulation.

Upon first inspection, the GDPR makes no material change to the general principle that consent is one way in which the processing of personal data can be legitimised and rendered lawful. However, if one is to analyse the GDPR's provisions relating to consent more thoroughly, particularly its recitals, it quickly becomes apparent that the GDPR makes it considerably more difficult for data controllers to obtain valid consent than is the case currently under the DPD or DPA.

In Recital 32, for instance, it is specified that consent can be expressed by:

> "*…a written statement, including electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services, or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of his or her personal data*."

It is also made clear in Recital 32 that:

> "*Silence, pre-ticked boxes, inactivity, a failure to opt-out, or passive acquiescence do not constitute valid consent.*"

Recital 42 then states that:

> "*Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation.*"

That:

> "*Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.*"

That:

> "*…a declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms*."

And that:

> "*For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.*"

Recital 43 further specifies that:

> "*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority…*"

From this overview of the GDPR's provisions relating to consent, we can identify several notable ways in which obtaining valid consent is a more demanding task under the GDPR than is presently the

case under the DPD or DPA. This is something that has been acknowledged in the data protection literature, with various observers noting the GDPR's stricter consent requirements.[98]

The first obvious difference between the GDPR and the DPD is the fact that whilst under the DPD the data subject is required to "*signify*" their consent for it to be considered valid, under the GDPR the data subject will be required to express their consent by way of a "*statement or clear affirmative action*". The obvious implication of this being that future consents must be obtained on an "opt-in", rather than "opt-out", basis if they are to be considered valid.

Secondly, whilst the DPD sheds very little light on the meaning of the phrase "*freely given*", with most guidance in relation to this term coming in the form of Article 29 Working Party opinions, the GDPR makes it considerably more challenging for data controllers to demonstrate that any consents obtained have been given freely. Particularly, as noted above, under the GDPR data controllers are obliged to ensure that all data subjects have a "*genuine choice*" in respect of any prospective consent transactions to which they are subject, and to observe a general presumption that consents cannot be freely given, and therefore cannot form the legal basis for the processing of personal data, where there is a clear imbalance between the data subject and the data controller.

From the text of the GDPR itself, it is not immediately obvious what is meant by the term "*imbalance*". Some guidance as to its meaning can be found, however, in the recently published ICO draft guidance on the GDPR's consent requirements.[99] Particularly, the ICO advises that an imbalance of power will exist when an individual is reliant on another party for the provision of services, or fears adverse consequences linked to the withdrawal of those services, and feels they have no choice but to agree to whatever terms the services provider offers. Specifically, the ICO notes that relationships between employers and employees, as well as relationships between individuals and public authorities, are those in which a clear imbalance of power is likely to exist between the involved parties.[100]

In other words, it would appear that an imbalance of power will be present where there is an observable inequality of bargaining power between two or more parties, due to the level of influence one has over the other.[101] It would therefore appear that the notion of "imbalance" in the immediate context is comparable to its usage in other areas of EU law, notably those which deal with consumer protection.[102] In the fields of consumer and competition law, however, various observers have noted an apparent reluctance of the CJEU to articulate minimum standards of fairness and consumer

[98] See, for example: Schermer, B. et al. (2014) "The crisis of consent: how stronger legal protection may lead to weaker consent in data protection", *Ethics and Information Technology* 16(2), pp.171-182; van der Sloot, B. (2014) "Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation", *International Data Privacy Law* 4(4), pp.307-325.

[99] ICO (2017) *Consultation*: *GDPR consent guidance*. Available at: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

[100] *Ibid*., pg.14.

[101] To this end the ICO guidance can be said to correlate with earlier UK jurisprudence regarding the doctrine of inequality of bargaining power. See, for example: *Schroeder Music Publishing Co Ltd v Macaulay* [1974] 1 WLR 1308, 1316.

[102] Article 3 of Directive 93/13/EEC on unfair contract terms in consumer contracts specifies, for instance, that a contractual term which has not been negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.

protection, which, in turn, has impeded the development of a comprehensive understanding of the concept.[103]

In any event, as noted above, and as is alluded to by both the ICO guidance the GDPR itself, imbalances of power are likely to be particularly prominent in situations in which the data controller is a public authority.[104] Significantly in this regard, however, though the GDPR makes numerous references to public authorities throughout its text, "public authority", like "imbalance", is a term that is not fully defined at any point.[105] Some guidance as to its meaning can, however, perhaps be inferred from CJEU case law outside the data protection field. When addressing matters concerning the doctrine of direct effect in *Foster v British Gas*,[106] for instance, the CJEU considered the notion of "emanation of the state", and remarked that it was a term that should be taken to refer to:

> "*...a body, whatever its legal form, which has been made responsible, pursuant to a measure adopted by the State, for providing a public service under the control of the State and has for that purpose special powers beyond those which result from the normal rules applicable in relations between individuals...*"[107]

Though the terms "emanation of the state" and "public authority" are not necessarily synonymous with one another, it seems highly probable that the former is broad enough to encompass the latter.

More recently, however, in *Fish Legal*[108] the CJEU specifically considered the meaning of "public authority" in the context of the Public Access to Environmental Information Directive,[109] which requires public authorities to provide environmental information upon request.[110] Here, it was remarked that in order to determine whether a body constitutes a public authority it should be examined whether it possesses "*special powers beyond those which result from the normal rules applicable in relations between persons governed by private law*".[111] The possession of such "special powers", therefore, would likely indicate that a body was a public authority. The Court further observed that if a body is incapable of acting in a genuinely autonomous fashion, and that it cannot

[103] See, for example: Schillig, M. (2008) "Inequality of Bargaining Power Versus Market for Lemons: Legal Paradigm Change and the Court of Justice's Jurisprudence on Directive 93/13 on Unfair Contract Terms", *European Law Review* 33, pp.336-358. The ambiguity of the term has also been considered in the context of EU competition law. See: Akman, P. (2012) *The Concept of Abuse in EU Competition Law: Law and Economic Approaches*, Oxford: Hart, pg.162.
[104] n.99. pg.14.; Recital 43 General Data Protection Regulation.
[105] As an interesting point of comparison, however, s.1(1) of the UK Data Protection Act 1998 states that the term "public authority" in the data protection context should be defined in the same way as it is defined by Schedule 1 of the UK Freedom of Information Act 2000, which states that, amongst other institutions, government departments, The Competition and Markets Authority, The Office for Standards in Education, Children's Services and Skills, The Houses of Parliament, The Northern Irish and Welsh Assemblies, the armed forces, and local authorities should all be considered public authorities.
[106] Case C-188/89 Foster v British Gas Plc, EU:C:1990:313.
[107] *Ibid*., at 22.
[108] Case C-279/12 Fish Legal and Emily Shirley v ICO and Southern Water, United Utilities and Yorkshire Water, EU:C:2013:853.
[109] Officially known as Directive 2003/4/EC of the European Parliament and of the Council on public access to environmental information and repealing Council Directive 90/313/EEC. L.41/26.
[110] *Ibid*., Article 3.
[111] Case C-279/12 Fish Legal and Emily Shirley v ICO and Southern Water, United Utilities and Yorkshire Water, EU:C:2013:853, at paragraph 52.

demonstrate that its provision of services is free from decisive influence of any governmental or public administrative organisations, this would also likely indicate that it was a public authority.[112]

Further guidance as to the meaning of the term may also be found in the text of, and case law relating to, the Human Rights Act 1998,[113] the statute responsible for incorporating the terms of the European Convention on Human Rights[114] into the UK's domestic legal order. Significantly, Section 6 of the HRA states that it will be unlawful for a public authority to act in a way that is incompatible with any of the rights contained in the ECHR,[115] and specifies that the term "public authority" will encompass any court or tribunal,[116] as well as any person certain of whose functions are functions of a public nature, not including the Houses of Parliament or any person involved in parliamentary proceedings.[117] Other than this general guidance, however, it has been left to UK Courts to identify and determine the identity of public authorities. The leading case in this regard is *Aston Cantlow Parochial Church Council v Wallbank*.[118] Here the House of Lords suggested that the central characteristic of a public authority would be an ability to act in a way that was "*governmental in the broad sense of that expression*".[119] It appears that the test for whether a body constitutes a public authority in this context, therefore, is not whether the body in question is owned or operated by the state, but whether it performs a function that can be considered governmental in nature. In subsequent cases it has since been suggested that functions are likely to be considered governmental if they involve the exercise of coercive or other particularly intrusive powers, which would ordinarily, but not necessarily exclusively, be based on statute.[120] Conversely, it would appear that functions exercised on the basis of private contractual relationships are unlikely to be deemed governmental. Notably the UK Data Protection Bill includes a limited list of public authorities in its section 6 and refers specifically to section 3 of the Freedom of Information Act 2000[121] for this purpose.

Thirdly, whilst the DPD fails to provide any details or guidance on the methods that can be used to obtain valid consent, the same cannot be said in respect of the GDPR. As noted above, the GDPR specifically recognises the validity of several methods that may be utilised by data controllers as a means of obtaining consent, ranging from verbal statements and written statements, to the ticking of boxes and the adjustment of technical settings. In so doing, the GDPR endorses the sentiment that different methods for obtaining consent may be more suitable than others in certain contexts, and compels data controllers to pick those that are most suitably aligned to their data processing practices. It is further made expressly clear that complete inaction or passive acquiescence on behalf of the data subject will never amount to genuine consent.

One final significant difference between the DPD and the GDPR relates to data controllers being able to demonstrate that they have obtained valid consent from data subjects. Whilst the DPD does not explicitly contain any requirement that data controllers must maintain evidence of any consents obtained from data subjects, the GDPR makes it clear that data controllers are formally required to be

[112] *Ibid*., paragraphs 68 and 71.
[113] [hereinafter HRA]
[114] Officially known as the Convention for the protection of Human Rights and Fundamental Freedoms [hereinafter ECHR].
[115] S.6(1) Human Rights Act 1998.
[116] *Ibid*., S.6(3)(a).
[117] *Ibid*., S.6(3)(b).
[118] *Aston Cantlow Parochial Church Council v Wallbank* [2003] UKHL 37.
[119] *Ibid*., Lord Nicholls at 7.
[120] See, for example: *YL v Birmingham City Council* [2007] UKHL 27.
[121] 2000 c. 36.

able to demonstrate that the consents they have obtained have been obtained validly. In situations in which a data subject and a data controller disagree as to whether consent has been validly given or obtained, therefore, the burden of proof will be on the data controller to demonstrate that this has occurred, which in turn will require an audit trail.

In addition to the apparently tightened rules regarding consent that can be found in the text of the GDPR itself, the abovementioned ICO draft guidance on the GDPR's consent requirements offers further clarification as to consent's interpretation.[122] Notably, and perhaps unsurprisingly, the ICO's draft guidance stresses that the words "unambiguous" and "clear affirmative action" in the GDPR's definition of consent must be interpreted as meaning that all consents must be obtained on an opt-in basis. The guidance, for instance, particularly warns against using pre-ticked boxes or similar methods of acquiring consent by default.[123] Additionally, the ICO guidance specifies that any organisation or third parties with whom data controllers intend to share personal data on the basis of an individual's consent must be explicitly named prior to the giving of consent in order for that consent to be deemed valid; the naming of specific sectors or categories of third parties will not be enough to sufficiently demonstrate compliance with the GDPR.[124] In a similar vein, it is also specified that where possible, individuals should be given granular options to consent, rather than being presented with very broad consent notices.[125]

Perhaps most interestingly, however, the ICO guidance specifically addresses the point that consent, as noted above, is only one of a number of legitimising grounds by which the processing of personal data can be rendered lawful, and that data controllers should only seek to rely on it in appropriate circumstances. In this respect, the guidance draws precise attention to the fact that, due to imbalances in power between parties, consent will, in the majority of circumstances, not be an appropriate legal basis for personal data processing operations undertaken by public authorities, and advises that public authorities should actively avoid relying on consent and seek to identify alternative legitimising grounds for the processing of personal data.[126]

3.3 Processing that is necessary for the conclusion or performance of a contract to which the data subject is a party

Both the DPD and GDPR specify that, other than relying on individual consent, the processing of personal data may lawfully occur when such processing is necessary either for entering or performing a contract with the individual to whom those data relate.[127] As has been noted elsewhere,[128] "necessary" is an adjective that appears frequently in other legislative instruments, notably the ECHR. Significantly in this regard, the jurisprudence of the European Court of Human Rights - which has been approved by the CJEU - has historically adopted an interpretation requiring that the practice in question be close to essential for the specified purpose.[129]

[122] n.99.
[123] *Ibid*., pg.3.
[124] *Ibid*
[125] *Ibid*
[126] *Ibid*., pg.14.
[127] See: Article 7(b) Data Protection Directive; Article 6(1)(b) General Data Protection Regulation.
[128] See, for example: Lloyd, I. (2017) *Information Technology Law*: Oxford: Oxford University Press, pg.108.
[129] See, for example: *Barthold v Germany* (1985) 7 EHRR 383.

The work of the Article 29 Working Party appears to suggest that a similar standard would be required in the data protection context if process personal data were to be processed on this basis.[130] In other words, in order to legitimately process personal data on this basis, it would appear that data controllers must be able to show that it would be essentially impossible to enter a contract, or perform a contractual duty in relation to a particular individual, without processing any of said individual's personal data. The requirement that the processing be "essential" should also probably be read together with the principle of data minimisation.

This legitimising ground is likely to be particularly relevant in situations involving a contractual agreement between an individual and a private party, such as a bank or insurance company. For instance, in order for a bank or insurer to be able to evaluate an individual's application for a loan or an insurance policy, the consideration of information such as the individual's name, date of birth and address will be integral to making such a determination.[131] Another salient example provided by the Article 29 Working Party is that the processing of personal data may in some situations be necessary for the performance of a contract of employment.[132] As others have suggested, however, this ground for the processing of personal data is perhaps of limited applicability in this context. Whilst it may, for example, be useful for an employer to record details of employees' next of kin in the event of accident or illness at work, this would not ordinarily be considered essential for the normal purposes of employment, and thus the identification of an alternative ground for processing would likely be required to render such a practice lawful.[133]

3.4 Processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

The European data protection framework also specifies that the processing of personal data is permissible when such processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest. Particularly, Article 7(e) DPD and Article 6(1)(e) GDPR both specify that processing will be lawful when it is:

> "*...necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*…"

Whilst neither the DPD nor the GDPR explicitly define the term "public interest", both legislative instruments allude to the fact that matters concerning public health, social protection, taxation and customs administrations, humanitarian issues would fall within its scope.[134] This is an understanding of the term that is also alluded to by the Art.29 Working Party.[135] The UK ICO has more rigorously examined the notion of "public interest" in the data protection context, and in its guidance on the public interest test in the context of the UK Freedom of Information Act 2000 states that:

---

[130] See, for example. Article 29 Working Party (2005) Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114. pp12-14.
[131] n.127. pg.108.
[132] Article 29 Working Party (2001) Opinion 8/2001 on the processing of personal data in the employment context, WP 48. pg.8.
[133] n.127. pg.109.
[134] See; Recitals 34 and 58 Data Protection DIrective; Recital 46 and Article 36(5) General Data Protection Regulation.
[135] Article 29 Working Party (2017) Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248. pg.18.

> "*The public interest can cover a wide range of values and principles relating to the public good, or what is in the best interests of society. Thus, for example, there is a public interest in transparency and accountability, to promote public understanding and to safeguard democratic processes. There is a public interest in good decision-making by public bodies, in upholding standards of integrity, in ensuring justice and fair treatment for all, in securing the best use of public resources and in ensuring fair commercial competition in a mixed economy…*"[136]

Section 7 of the UK Data Protection Bill, which as noted above has been drafted as a means of transposing the main terms of the GDPR into the UK's domestic legal order after "Brexit", is more concise and states that the processing of personal data will be deemed to be in the public interest if it is:

> *"necessary for the administration of justice, the exercise of a function of either House of Parliament, the exercise of a function conferred on a person by an enactment, or the exercise of a function of the Crown, a Minister of the Crown or a government department."*

More broadly, away from the data protection field, notably in the context of issues relating to the free movement of goods, services, persons or capital, the CJEU has considered the term, amongst other things, to encompass matters relating to: the protection of public health, the protection of consumers, the protection of the environment, ensuring the integrity of the financial sector, the prevention of crime, the maintenance of financial and competitive balance, and the need to ensure the proper functioning of sporting competitions.[137]

Irrespective of the definition of public interest itself, however, it is important to note that any processing of personal data undertaken on this basis may be subject to objections from the individuals whose personal data are involved.[138] Once again, it is also important to pay heed to the DPD and GDPR's inclusion of the term "necessary". A clear apparent implication of this being that the processing of personal data in pursuit of performing a task that is in the public interest will not be permissible unless the achievement of said task cannot be achieved without the processing of personal data, and said processing cannot be legitimised by other means, such as the consent of the affected individuals.

3.5 Processing that is necessary for the purposes of the legitimate interests of the data controller or other third party

The final legitimising ground for the processing of personal data listed by both the DPD and the GDPR is possibly the most extensive, and perhaps also the most controversial. It sanctions the processing of personal data where it is necessary for the purposes of the legitimate interests pursued

---

[136] ICO (2017) *The public interest test: Freedom of Information Act*, pp.5-6. Available at: https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf

[137] See, for example: Case 120/78 Cassis de Dijon, EU:C:1979:42; Case C-368/95 Familiapress, EU:C:1997:325; Case C-415/93 Bosman, EU:C:1995:463; Case C-325/08 Bernard, EU:C:2010:143; Case C-55/94 Gebhard, EU:C:1995:411; Case C-288/89 Gouda, EU:C:1991:323; Case C-367/98 Commission v Portugal ("Golden Shares"), EU:C:2010:669; Case C-138/02 Collins, EU:C:2004:172.

[138] See: Recital 69 General Data Protection Regulation. See also Articles 18 and 21 General Data Protection Regulation.

by the data controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.[139]

Whilst the DPD says little in respect of the meaning of "legitimate interests", the recitals of the GDPR offer some insight as to its interpretation. Recital 47, for instance, specifies that a legitimate interest could exist where there is a "relevant and appropriate" relationship between the data subject and data controller, such as situations in which the data subject is a client of, or in the service of, the controller.

As specific examples the Recital also states that the processing of personal data for the purpose of preventing fraud "constitutes a legitimate interest" and the processing of personal data for the purpose of direct marketing may be regarded as being carried out for a legitimate interest. However, in the Recital it is also made clear and emphasised that the legitimate interests of data controllers could be overridden by the fundamental rights of individual data subjects in situations where said individuals do not reasonably expect their personal data to be processed.[140] In other words, any processing of personal data that is undertaken on the basis of the legitimate interests of the data controller will not be considered valid if said legitimate interests are outweighed by a need to protect the fundamental rights of individual data subjects whose personal data are involved. In this respect it is important to note, therefore, that determining the existence of a legitimate interest will require a careful assessment in respect of any potential balancing that may be required in relation to any competing fundamental rights of affected individuals.

As another interesting caveat, Article 6(1) of the GDPR also makes it clear that this ground for personal data processing will not apply to processing carried out by public authorities in the performance of their tasks. In this respect, however, the abovementioned possible ambiguities inherent in the term "public authority" must be kept in mind. Similarly, the abovementioned restrictions associated with the adjective "necessary" must also be remembered.

The legitimate interest concept has also been considered by both the Article 29 Working Party and the CJEU. In a 2014 opinion on the legitimate interests of data controllers, for instance, the Article 29 Working Party clarified both the words "legitimate" and "interest" in the data protection context. The Working Party first suggested that "interest" is not a term that is synonymous with "purpose". According to the Working Party, in data protection discourse the "purpose" of a data processing activity is the reason or aim why any data are processed. Conversely, an "interest" is the benefit that may be derived from that processing.[141]

Secondly, the Working Party suggested that the notion of a "legitimate interest" is broad, but highlighted some of the most common situations in which legitimate interests within the data protection field may arise. These included: the exercise of the right to freedom of expression; conventional direct marketing; unsolicited commercial messages; the enforcement of legal claims and debt collections; the prevention of fraud; employee monitoring; and the processing of personal data for historical, scientific or statistical purposes.[142]

[139] See: Article 7(f) Data Protection Directive and Article 6(1)(f) General Data Protection Regulation.
[140] The possibility of individual data subjects objecting to their personal data being processed on the basis of the legitimate interests of a data controller is also explicitly mentioned by Recital 69 of the GDPR.
[141] Article 29 Working Party (2014) Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217. pg.24.
[142] *Ibid*., pg.25.

In summation of the above points, the Working Party advised that in order to be relevant under data protection law, a legitimate interest must be: lawful (i.e. in accordance with applicable EU and national law); sufficiently clearly articulated to allow a balancing exercise to be carried out in relation to the interests and fundamental rights of affected individuals; and must represent a real and present interest, as opposed to an interest that is purely speculative.[143]

In the same opinion the Working Party also advised that any balancing assessment a data controller undertakes in relation to their own legitimate interests and the fundamental rights of individuals should not in any way be thought of as straightforward, nor a case of merely attempting to weigh and balance two easily calculable and comparable values. In this vein, the Working Party explicitly warned against data controllers treating the legitimate interests condition as an "*open door*" to legitimise their data processing activities.[144]
Instead, the working party suggests that making such a determination requires an extensive consideration of a number of factors, such as the nature and source of the data controller's legitimate interest, the potential impact the proposed processing would have on the individual or individuals whose data were involved, and the existence or presence of any additional safeguards which could limit undue impact on these individuals, such as privacy enhancing technologies, increased transparency, rights to opt-out, and the right of data portability.[145] This advice on the potential complexity of making such assessments correlates strongly with what was said on the matter by the UK ICO in its 2014 discussion paper on big data and data protection.[146]

More recently, in *Rīgas satiksme,*[147] the CJEU also examined the legitimate interests ground for personal data processing. Particularly, the court considered the meaning of the term "necessary" and the question of whether the legitimate interests ground for data processing imposes obligations on data controllers to disclose the personal data of an individual to a third party for the purposes of allowing said third party to initiate legal proceedings against that individual.

The conclusion arrived at by the CJEU was that the disclosure of an individual's personal data in such a scenario on the basis of the legitimate interests ground for processing would only be permissible in cases where the fundamental rights of that individual do not take precedence. The CJEU also concluded that the legitimate interests ground for processing does not impose any obligations on data controllers to disclose personal data to third parties in situations similar to that mentioned above, but merely permits them to make such disclosures in accordance with the national laws of the Member State in which they are based.

Of particular interest were the remarks of AG Bobek, who suggested that the concept of a legitimate interest was "*elastic enough*" to encompass considerations other than a need to protect property, health, and family life, specifically identifying the issuing of a legal claim as a particular example.[148] The AG also seemingly re-emphasised the earlier guidance of the Article 29 Working Party by suggesting that as a part of any attempts to balance the legitimate interests of a data controller with the

[143] *Ibid*
[144] *Ibid*., pg.49.
[145] *Ibid*., pg.33.
[146] ICO (2014) *Big data, artificial intelligence, machine learning and data protection*, pg.33. Available at: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf
[147] Case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme',* EU:C:2017:336.
[148] *Ibid*., at paragraph 65.

fundamental rights of an individual "*due consideration should in particular be given to the nature and sensitivity*" of the data involved.[149] In his concluding remarks the AG also suggested that whilst the original and primary purpose of data protection law is the regulation of large-scale datasets involving personal data, "*a much lighter touch*" would be called for in situations involving datasets of a lesser size or individual pieces of information.[150] In so doing, the AG's comments appear to endorse a position of pro-active reliance on the legitimate interests ground for personal data processing in appropriate circumstances. As has been remarked elsewhere, for instance, this position might be said to sit somewhat uneasily with the abovementioned Article 29 Working Party opinion, which urges data controllers not to think of the legitimate interests condition as an open door to legitimise their data processing operations.[151]

3.6 Gov.UK Verify and its dual legal basis

The study of the content of the DPIA concluded in 2016 shows that Gov.UK is intended to be grounded upon two and not one legal basis,[152] although in public communications targeting service users in particular consent has probably been presented as being the main legal basis. While the legal basis corresponding to the *"processing that is necessary for the task carried out in the public interest or in the exercise of official authority vested in the controller"* does not seem to raise any concern, consent as the second (or probably first) legal basis creates some difficulties.

One key question is thus whether consent is a valid legal basis for the processing undertaken by identity providers. First, one could note that there is potentially free choice for data subjects as both identity providers and service providers should offer alternative means to access their services. Besides, the explanation found below the description of the first identity assurance principle stresses that *"*[f]*ailing to do so would undermine the consensual nature of the service."*[153]

However, one could argue that despite the fact that these identity providers are private companies there should be a presumption of a clear imbalance between the data subject and the controller in the same way as there seems to be a presumption of a clear imbalance between data subjects and public authorities. It is evident, for instance, that there is a very intimate relationship between identity providers and the GDS. This raises the question as to whether identity providers could be assimilated into public authorities even though they could not be described as such as per the definition contained within the Freedom of Information Act.

There are several reasons as to why it may be possible to answer this question in the positive. First of all, identity providers are certified by the GDS.[154] Second, identity providers are actually paid by the GDS.[155] Third, the relationship between identity providers and the GDS is regulated through the means of a complex framework agreement, which is made up of a range of stipulations relating to

[149] *Ibid*., at paragraph 69.
[150] *Ibid*., at paragraph 98.
[151] Knight, A. (2017) "CJEU Advocate General Opines on the 'Legitimate Interest' Concept", Inforrm Blog, available at: https://inforrm.wordpress.com/2017/02/05/cjeu-advocate-general-opines-on-the-legitimate-interest-concept-alison-knight/
[152] DPIA, pg. 10 and pg. 25.
[153] n.62. pg.8.
[154]
[155] Framework agreement, section D.

reports, records and monitoring by the GDS.[156] Interestingly, in most other Member States, the verification of identity is undertaken by public authorities. Out of the ten countries currently operating eID schemes, four use only public eID means, whereas in four others public and private means co-exist. Although in many the construction of the infrastructure and the means (e.g. the cards) happens by private entities (through tenders), authentication is usually operated by the government. Only two countries (the UK and Denmark) have opted for exclusively private means (due in part to the lack of governmental ID cards).

Country	Classification of eID means	Comments
Austria	Public	Multi-means (mix of public and private) eIDs, such as governmental eID cards and (private) mobile eIDs. Issuing of eIDs is always a governmental task. Certificates come from a private certification authority (under supervision of the government). The market fulfils subsequent roles (e.g. mobile eID means) as long as they meet the government's standards.
Belgium	Public	Identity and identification under governmental control (through an eID card). Private parties were involved through tenders in the realisation of the infrastructure, but the means remain under government's control.
Denmark	Private	Denmark does not have a national ID card. Therefore, eID is provided from the private sector through five-year long tenders.
Estonia	Public and private	Estonia operates a governmental eID card but several banking cards with eID functions co-exist. The public eID card allows for more transactions than the banking cards due to the higher assurance level it offers.
France	Public (unimplemented)	France has designed a public eID card which was rejected by the French Constitutional Council. No alternative means are currently in the works.
Germany	Public	In Germany, identification, including eID, falls exclusively within the domain of the public sector. The means used is an official eID card (that doubles as an offline ID document). Private parties are involved in the production of the cards, but their use and operation is controlled by the government.
Luxembourg	Public and private	Traditionally eID provision was administered by way of a public-private partnership, LuxTrust, with the government owning two thirds of the shares. Recently, however, Luxembourg has begun the rollout of a public eID card.
Portugal	Public	The Portuguese eID scheme operates with a public

156

		eID card (that serves also offline ID purposes).
Spain	Public (and public and private)	At present there are two eID schemes operating in Spain: a nationwide public eID card and a certificate-based card that uses a mix of public and private means. The alternative certificate-based scheme is not recognised in all regions of Spain.
Sweden	Public and private	The Swedish eID scheme was previously exclusively based on banking cards. Concerns in respect of the lack of inclusivity of this arrangement, however, have led to the introduction of a public eID card, offered by a public carrier. The two means of eID now co-exist under the same scheme.
UK	Private	In the UK authentication is operated by private sector actors, selected by the government through a tender. The actors not only carry out the authentication, but also verify the identity of the users themselves.

Table 3: eID schemes country profiles[157]

If we are to assume that there is such a thing as a European concept of public authorities (which should be independent from any competing national definitions)[158] there is an argument that companies certified by the GDS should also be considered public authorities themselves. As noted above, for instance, the jurisprudence of both the CJEU and UK courts suggests that any bodies or institutions, irrespective of their legal form, that are responsible for providing a public service on behalf of the state, are afforded special powers or competencies by way of their relationship with the state, or are unable to act autonomously and in a way that is free from decisive influence of the state, must be considered public authorities. Companies certified by the GDS could arguably be described as possessing some, if not all, of these characteristics.

Consent as a legal basis becomes even more problematic when used directly by (government) service providers. As touched upon above, to the question whether *"suppliers/partners have the right to use the personal information collected or shared under the service for their own purposes"*[159] the answer appears to be that *"Government Services may use information for their own purposes, but will have to disclose purposes and details of information required to the service user on a per-transaction basis, and seek appropriate consent."*[160]

[157] Adapted from PBLQ, International Comparison eID Means (Final report, version 1,0, 10 April 2015) (last accessed October 2017) pp.14-18. https://kennisopenbaarbestuur.nl/rapporten-publicaties/international-comparison-eid-means/

[158] As a general principle of EU law, many of its key constituent elements and concepts across various areas of law are intrinsically based in EU law itself and, as a necessary corollary, are not based on national definitions which exist in the domestic legal order of EU Member States. See, for instance, the treatment of the definition of "worker" in "Commuication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions Reaffirming the free movement of workers: rights and major developments", *COM/2010/0373 final*.

[159]

[160]

Assuming consent cannot operate as the legal basis for the processing of personal data between service users and identity providers we are thus left with the performance of a task carried out in the public interest, unless the legal basis corresponding to the conclusion or performance of a contract could also potentially be relied upon, assuming there is a contract between the certified companies and the service users.

From the analysis of the doctrine of legal bases undertaken above, it appears that the role given to consent under the GDPR has expressly been curtailed in comparison to its role within the DPD. As a result, it is arguable whether consent could be used at all to legitimise the processing of personal data by identity providers. Suspicions towards consent as a legal basis rise significantly when one allocates data protection roles to the four actors identified in the second section: GDS, (government) service providers, identity providers and service users. This is mainly due to the way in which the relationship between the GDS and the identity providers could be characterised as a situation of joint controllership in relation to the personal data processing activities undertaken by the identity providers themselves.

4. Choosing the appropriate legal basis in a situation of joint controllership

Having considered the grounds substantive legitimising grounds for the processing of personal data in the previous section, as well as their potentially applicability to GOV.UK Verify, this section of the article explains the doctrine of joint controllership, distinguishes it from the more orthodox processor-controller relationship that is typically inherent in many contemporary data-handling practices, and then analyses to what extent eIDAS frames the relationships of the different parties to an eID scheme. The ecosystem of GOV.Uk Verify is then assessed in light of these considerations.

4.1 The doctrine of joint controllership

The DPD does expressly acknowledge the possibility of having situations of joint controllership. It uses the expression *"alone or jointly with others"* and provides that a data controller is:

> *"...the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law."*

The Article 29 Working Party in its opinion on the concepts of "controller" and "processor"[161] attempts to provide some guidance on the notion of processing that is undertaken "alone or jointly with others" and refers back to the opinion of the Commission on the European Parliament to explain that a situation of joint controllership can exist even in situations in which the data controllers do not *"equally"* determine the means and purposes of a *"single processing operation."*[162]

Furthermore, the Working Party also confirms that the approach that should be used for categorising joint controllership should be the same as that used for characterising situation of sole controllership:

[161] Article 29 Working Party (2010) Opinion 1/2010 on the concepts of "controller" and "processor", WP 169
[162] *Ibid*, pg. 18.

"a substantive and functional approach,... focusing on whether the purposes and means are determined by more than one party."[163]

However, whilst at the beginning of its analysis the Working Party appears to consider that each data controller shall contribute to both the determination of the means and the purposes of the processes, it modifies its analysis, and specifies a few lines later that a party should be categorised as a controller if it is able to determine *either* the purpose or the essential elements of the means of an act of personal processing, as opposed to both:

> *"In this perspective, joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller."*[164]

In other words, a data processor should only ever be considered a joint controller if it determines the purpose or the "essential elements" of the means that characterize a controller.[165] A considerable variety of situations of joint controllership could thus be imagined.[166] Such a situation is perhaps particularly likely to arise when *"different actors would decide to set up a shared infrastructure to pursue their own individual purposes."*[167]

The Working Party then goes on to distinguish between two complementary approaches that are both relevant in order to determine whether a joint controllership situation exists in a particular scenario: a micro-level approach and a macro-level approach. In the words of the Working Party:

> *"In some cases, various actors process the same personal data in a sequence. In these cases, it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means."*[168]

In a chain of processing activities, the pursuance of a *"joint purpose"* thus appears crucial for the characterisation of a situation of joint controllership. Consequently, joint controllers are jointly responsible for any personal data processing operations relevant to that purpose.

As an interesting point of reference, a typology of the various different types of relationships between data controllers, co-controllers, and processors developed in 2005 by Olsen and Mahler, encompasses the majority of the types of collaboration envisaged by the Working Party in its guidance.[169] Particularly, it identifies that joint controllers will primarily come in two forms: partly joint

[163] *Ibid*
[164] *Ibid*, pg. 19.
[165] As has been noted elsewhere, however, the Working Party's distinction between "essential" and "non-essential" means appears to conflict with the definition of "Controller" found in Article 2(d) of the Data Protection Directive. See: Van Ecke, P. and Truyens, M. (2010) "Privacy and Social Networks", *Computer Law & Security Review* 26(5), pg.539.
[166] n.160, pg. 19.
[167] *Ibid*
[168] *Ibid*, pg. 20.
[169] Olsen, T. and Mahler, T. (2005) "Privacy - Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems", *Legal IST project*, pp.40-47.

controllers and fully scope joint controllers. A partly joint controller would be present where the purpose and means of a certain processing operation is determined jointly by more than one controller, while others are performed separately under the sole control of another controller, whereas a controller could be considered a full-scope joint controller if it and another controller jointly determine all the purposes and means of a particularly data processing operation.[170] This clarification aside, however, some observers have suggested that the notion of joint controllership remains a vague and confusing concept, particularly in certain contexts.[171]

What is also interesting is the way in which the Working Party directly mentions the example of e-government portals as a specific example of a platform that would fall within the definition of joint controllership. This is because e-government portals tend to involve various actors jointly determining *"the purposes and/or the means of a processing operation."*[172] For the sake of clarity, it is worth repeating Working Party's justification of its position in full:

> *"E-Government portals act as intermediaries between the citizens and the public administration units: the portal transfers the requests of the citizens and deposits the documents of the public administration unit until these are recalled by the citizen. Each public administration unit remains controller of the data processed for its own purposes. Nevertheless, the portal itself may be also considered controller. Indeed, it processes (i.e. collects and transfers to the competent unit) the requests of the citizens as well as the public documents (i.e. stores them and regulates any access to them, such as the download by the citizens) for further purposes (facilitation of e-Government services) than those for which the data are initially processed by each public administration unit. These controllers, among other obligations, will have to ensure that the system to transfer personal data from the user to the public administration's system is secure, since at a macro-level this transfer is an essential part of the set of processing operations carried out through the portal.*

Although this explanation was written in 2010, when GOV.UK Verify was not even in its infancy, and most the existing eID schemes were centralised and run by public authorities,[173] it may be premature to conclude that the position will necessarily be different when it comes to determining the categorisation of federated eID schemes.

What is also important in the context of joint controllership the fact that if a situation arises where one data controller is not in a position to meet all of its obligations as a data controller, and that another of its joint controllers is better place to perform certain data controller obligations, this will not prevent the involved parties from being categorised as joint controllers.[174] Furthermore, the Working Party insists that the lack of transparency in respect of the allocation of roles between different data

[170] *Ibid*
[171] Mäkinen, J. (2015) "Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things", *Information and Communications Technology Law* 25(3), pp.262-277.
[172] n.160, p. 21.
[173] In its 2011 report, the OECD notes that out of the 16 countries examined, 12 were operating centralised registration eID policies: OECD (2011) *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, pg.44. available at: http://www.oecd.org/sti/ieconomy/49338380.pdf
[174] n.160, pg. 22.

controllers can lead to an infringement of the principle of fair processing.[175] This is a position that has been implicitly endorsed by the UK ICO.[176]

The GDPR goes further than the DPD: not only is the GDPR more explicit in its recognition of situations of joint controllership, but also, as is explained in the next section of this article, it expressly derives the consequences of such a characterisation in terms of liability. For now, however, it is sufficient to note that the GDPR imposes an obligation on joint data controllers to determine their roles and responsibilities in a transparent manner so to ensure GDPR compliance. The terms of the GDPR appear particularly concerned with ensuring compliance with data subject rights, such as the right to information, *"unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject."*[177]

With all that has been said above in mind, the choice between a characterisation of a situation joint controllership and a processor-controller relationship is not necessarily a straightforward exercise. After having recalled the two cumulative criteria for qualifying an actor involved in the processing of personal data a processor that originates from DPD Article 2(e),[178] i.e. being an entity separate from the controller and processing personal data on behalf of the controller, the Article 29 Working Party offers a bundle of indicators to identity a processor-controller relationship:

- The range of the margin of manoeuvre left to the processor as a result of the instructions of the controller
- The modalities of the monitoring undertaken by the controller to supervise the activity of the processor
- The information provided by the controller to data subjects in relation to the allocation of roles between the different parties and thereby the expectations of data subjects as a consequence of this information
- The degree of expertise of each party[179]

However, the Working Party also insists upon placing a great deal of focus the complexity of processing activities, which can lead, perhaps prematurely, to prefer the characterisation of a situation of a joint data controllership rather than a processor-controller relationship, when combined with an assessment of the privacy risks:

> *"…the complexity of processing operations may lead to put more focus on the margin of manoeuvre of those entrusted with the processing of personal data, e.g. when the processing entails a specific privacy risk. Introducing new means of processing may lead to favouring the qualification as data controller rather than data processor. These cases may also lead to a clarification - and appointment of the controller - explicitly provided for by law."*[180]

[175] *Ibid*, pg. 24.
[176] See: n.84. pp.8-9; ICO (2014) *Data controllers and data processors: what is the difference and what the governance implications are*, pg.6. Available at: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf
[177] Article 26(1), GDPR.
[178] n.160, pg. 25.
[179] *Ibid*, pg. 28.
[180] *Ibid*, pg. 29.

Taking the example of processing activities undertaken for historical, scientific and statistical purposes, including anonymisation practices, Article 29 WP specifies that when data coming from different sources are combined together, *"there is a particular threat to data protection, justifying the intermediary organization's own responsibility.*"[181]

Because with the GDPR, the demarcation between the roles of processor and controller become less clear as processor's obligations have been multiplied and the status of processor made closer to that of controller, one could make the argument that the balance should be tipped in favour of a characterisation of a situation of joint controllership. This is a proposition that has been alluded to in the data protection literature, albeit with some observers suggesting that the blurring of boundaries between data controllers and data processors caused by technological evolution could lead to the emergence of a "confused" approach to data protection.[182]

That joint controllers should be considered to be joint and severally liable is a not a novelty unique to the GDPR. Despite the silence of the DPD, the Article 29 Working Party in 2010 interpreted the DPD as implying that the default rule under the DPD was that of joint and several liability.[183] However, the GDPR offers a more radical solution than the one anticipated by the Working Party. This is because even when joint controllers determine in a transparent manner their roles and responsibilities for the purposes of ensuring compliance with the GDPR, joint data controllers remain jointly and severally liable. GDPR Article 26(3) provides that: *"Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers."* Reading Article 26(3) together with Article 82(3) it appears that one joint controller will only be able to escape liability for the actions of another if it can demonstrate that "*it is not in any way responsible for the event giving rise to the damage*".[184]

4.2 eIDAS partition of roles

As alluded to above, eIDAS identifies the main actors of an eID scheme and their roles in the process of identification and authentication. However, significantly, eIDAS adopts a technologically neutral approach and does not attempt to dictate the way eID schemes should be designed.[185] Concurrently, if one is to examine the various national eID schemes that have been deployed to date in EU Member States, there is an observable variety in respect of their technological architectures. This was something that was recognised during the preliminary work leading up to the enactment of eIDAS.

In 2013 a feasibility study conducted as part of the EU IAS project noted that eID solutions "*were heterogeneous from a technology perspective, using smartcards […], Mobile eID's […], allowing soft*

[181] *Ibid*, pg.30.
[182] See, for example: Blume, P. (2013) "Controller and processor: is there a risk of confusion?", *International Data Privacy Law* 3(2), pp.140-145. See also: Kuan Hon, W. Millard, C. and Walden, I. (2012) "Who is responsible for 'personal data' in cloud computing? - The cloud of unknowing, Part 2", *International Data Privacy Law* 2(1), pp.3-18.
[183] n.160, pg. 22.
[184] Article 82(3) General Data Protection Regulation
[185] Article 12(3)(a) eIDAS provides that the interoperability framework aims *"to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State."*

certificates […], or even username/password […].”[186] It continued by stating that “*[m]ost solutions were established well before there was a common middleware standard*”.[187] This forced the STORK pilot, which formed the basis for eIDAS, “*to create a model that could accommodate the various existing models*.”[188] Along the same lines, the impact assessment accompanying the eIDAS proposal acknowledged a number of potential problems linked to issues concerning interoperability and cross-border interaction that could be posed by Member States using *“different technological solutions for personal identification*.”[189]

It is certainly true to say that eIDAS aims at supporting the creation of an interoperability framework to make cross-border transactions possible, and its implementation acts to some extent constrain its design.[190] However, per definition this is true only in the context of cross-border transactions and not in the context of internal transactions. This is because the interoperability framework has been conceived as a means to identify a minimum common denominator that could be accepted by all Member States without affecting the design or operation of their national eID schemes in relation to internal transactions. As a result, eIDAS should not be seen as a tool for comprehensively determining the roles and responsibilities of controllers involved in eID schemes.

What is true, however, is that by definition eIDAS specifies the purposes of the processing: identification and authentication, which should (although this is not explained in these terms in eIDAS), comprise two stages. The first being the creation of the electronic identification means from personal identification data, and the second being the subsequent use of the electronic identification means for authentication purposes. eIDAS gives a seemingly confusing account of this process in the sense that it seems to distinguish between identification and authentication, despite their definitions being very similar:

- Electronic identification: *“the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person.”*[191]

[186] European Commission, *Feasibility study on an electronic identification, authentication and signature policy (IAS)* (Final Version (D11b), Ref Ares(2013)2869715, 13 August 2013) p. 171.
[187] *Ibid*, pg. 172.
[188] *Ibid*.
[189] European Commission, *Impact Assessment Accompanying the proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market* (Commission Staff Working Paper, COM(2012) 238 final, 4 June, 2012), pg. 10.
[190] There have been arguments against the requirement of a Minimum Dataset (Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) [2015] OJ L 235 ANNEX) as well as a technical specification that would best serve central deployments and does not lend itself to newer technologies, such as zero-knowledge-credentials. See, for example, ABC4Trust Position Paper, 'Privacy-ABCs and the eID Regulation' 2014 <https://abc4trust.eu/download/documents/ABC4Trust-eID-Regulation.pdf> accessed 03 August 2015, pg. 2; Massacci, F. and Gadyatskaya,O. (2013) 'How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results' White Paper, pp.3-4. available at: http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf; Zwingelberg, H. and Schallaböck, J. (2013) 'H2.4 The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective' Opinion Paper, ABC4Trust EU Project, pp.9-10. Available at: https://abc4trust.eu/index.php/pub/deliverables/176-h2-4
[191] n.4. Article 3(1)

- Authentication: *"electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed."*[192]

As a result, it is not entirely clear whether electronic identification is a term that exclusively covers the creation of the electronic identification means, or if it also encompasses subsequent acts of authentication. That said, despite this imprecise language, the creation of the electronic identification means and confirming the identity of an individual through an electronic identification means are closely related activities, and will inevitably constitute acts of either electronic identification or authentication, if not both.

As mentioned above, eIDAS distinguishes between three actors: notifying Member States, parties issuing electronic identification means, and parties operating authentication procedures. eIDAS expressly recognises the fact that the electronic identification means can be issued by private parties. Article 7 therefore distinguishes three hypotheses: when the electronic identification means are issued by the notifying Member States, when they are issued under a mandate from the notifying Member State, or when they are issued independently of the notifying Member State but are recognised by that Member State.

The notifying Member State appears to be the one with the most obligations or duties. It shall ensure:

- *the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;*[193]
- *the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;*[194]
- *the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.*[195]
- *the cross-border authentication [is] provided free of charge when it is carried out in relation to a service online provided by a public sector body.*[196]

Parties operating authentication procedures do not seem, contrary to the text of eIDAS Article 11, to be subject to any specific obligation or duty.

Parties issuing electronic identification means shall ensure:

- *the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the*

[192] *Ibid*, Article 3(5)
[193] *Ibid*. Article 7(d)
[194] *Ibid*. Article 7(f)
[195] *Ibid*
[196] *Ibid*

relevant assurance level set out in the implementing act referred to in Article 8(3);[197]

This description appears to confirm, therefore, that the obligations and duties of eIDAS actors are broadly formulated and not necessarily data-protection related, but do cover personal data processing activities. At the same time, eIDAS is narrower in scope than the GDPR in that it only targets three types of actors.

Furthermore, Article 11 of eIDAS sets the liability rules applicable in cases in which the obligations and duties enumerated above are violated. Importantly, Article 11's liability rules are negligence based and do not specify any presumption of liability:

> *The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.*[198]

There is therefore a *prima facie* conflict between Article 11 of eIDAS and Articles 26 and 82 of the GDPR Articles 26 and 82. Ensuring a high level of data protection in the field of electronic identification would however require applying Articles 26 and 82 of the GDPR to matters involving the processing of personal data. This would mean that the conflict that exists between Article 11 of eIDAS and Articles 26 and 82 of the GDPR could not be alleviated by way of an argument that eIDAS is a sector-specific regulation in comparison to the GDPR. Accordingly, Article 11 of eIDAS derogates from Articles 26 and 82 GDPR. Instead, Articles 26 and 82 of the GDPR should still be applied to eID scheme actors. One way to accommodate this predicament would be to argue that eIDAS and the GDPR are complementary pieces of legislation, which would mean that a granular analysis and comparison of each of their respective provisions is necessary in instances where conflicts between appear to arise, in order to determine the most restrictive rules.[199] This route is preferable to arguing that the eIDAS is a sector-specific piece of legislation as its liability provisions are not the only provisions that could potentially be in conflict with those of the GDPR. In this respect it is also worth noting that eIDAS contains more restrictive rules in relation to breach notification obligations than the GDPR.[200]

Interestingly, the partition in the final version of eIDAS differs slightly from its draft text. Notably, in earlier drafts[201] of eIDAS rules relating to requirements imposed on Member States in relation to notifying the European Commission of their national eID schemes scheme lacked the phrase "*at the time the electronic identification means under that scheme is issued*".[202] Therefore, according to this wording, the Member State would have been constantly liable for the unambiguous attribution of personal identification data throughout the use of an eID (as opposed to just at the time of first issuance, which is the case under the final version). Under the same draft,[203] Member States were liable for the availability of user authentication "*at any time and free of charge*" and did not

[197] *Ibid*, Article 7(e)
[198] *Ibid*, Article 11(2)
[199] Liability provisions are not the only provisions that could potentially be in conflict. eIDAS contains more restrictive rules in relation to breach notification obligations.
[200]
[201] *Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Text with EEA relevance)* (COM(2012) 238 final, Brussels, 4 June 2012) Art. 6(1)(c).
[202] n.4 Art.7(d)
[203] n.200. Art. 6(1)(d).

discriminate between public-sector and private-sector relying parties. On the contrary, the final version of eIDAS allows Member States to "*define terms of access to that authentication*" and guarantees free of charge access to public-sector bodies only.[204] Lastly, the final version of eIDAS is more precise in respect of its provisions regarding the liability of participating parties,[205] with earlier drafts containing only liability provisions regarding Member States "*without prejudice to the liability of parties to a transaction in which electronic identification means falling under the notified scheme are used*."[206]

4.3 Gov.UK Verify and its segregation of roles and responsibilities

It is true that the DPIA attempts to distinguish between two types of purposes in order to distinguish the processing activities of identity providers-certified companies from the processing activities of GDS. It is explained that *"GDS will process personal data for the purpose of matching Service Users to Government Service records."*[207] At the same time, *"*[p]*urposes for Certified Companies processing personal data are defined within the procurement documentation, and Certified Companies are obliged to clearly state purposes in their privacy notices."*[208] This seems to explain or justify why identity providers and GDS are both data controllers but for their respective processing activities a distinct legal basis needs to be identified.

However, a careful analysis of both the framework agreement and the reality of the practices show that the different processing activities are better described as a set of processing activities aimed at a common purpose: authentication.

While contractual arrangements are a useful tool to characterise the situation at hand, this does not mean that the qualifications retained by the parties should necessarily be retained. These qualifications should be confronted with the factual arrangement of the relationship.[209] The framework agreement, as aforementioned, specifies the purposes for the processing in its schedule 2(a) on services description: to *"provide the following online identity assurance services to users seeking to access any HMG Service, with the objective of allowing them to prove that they are who they claim to be to defined levels of assurance."*[210]

In addition, from the perspective of service users, i.e. data subjects, it is artificial to distinguish between the processing undertaken by identity providers, GDS and (government) service providers. The three types of processing activities aim to ensure the realisation of one process: authentication for a communicating with a (government) service provider.

The question is then whether for this set of processing activities identity providers should be categorised as processors or data controllers. It is true that under the framework agreement identity providers are imposed security obligations,[211] obligations to ensure data subjects can exercise their

[204] n.4.Art. 7(f)
[205] *Ibid*, Art. 7(e) on the responsibility of the issuing party is a new addition; as well as Art. 11(2) and (3), ibid n. 4.
[206] n.200. Art. 6(2).
[207] Government Digital Service, *Gov.UK Verify Data Protection Impact Assessment* (n. **Error! Bookmark not defined.**), pg. 24.
[208] *Ibid*, pp. 24-25.
[209] n.161. pg.18.
[210] Cabinet Office, *Framework Agreement and Schedules* (n. **Error! Bookmark not defined.**), sch. 2 (part 2(A1)). See also clause 13.1.
[211] *Ibid*, clause 17.4.

rights,[212] reporting obligations in favour of GDS,[213] an obligation to request authorisation for the transfer of personal data to third countries,[214] an obligation to appoint any material sub-contractor,[215] and obligations relating to the training of identity providers' personnel.[216] It is also worth noting that a monitoring and supervision mechanism is put in place.[217] In any event, GDS is meant to review each certified company's privacy notice.[218]

As the GOV.UK Verify DPIA confirms, the set of processing activities inherent in the use of the service are extremely complex and necessarily require the data from a variety of sources, some of which should be considered highly sensitive, such as authentication credentials and transactional data. However, when it comes to authentication credentials, only service users and identity providers retain them. Besides, identity providers also have access to citizen verification data, i.e. *"information about or from passports and driving licences* (...) *commonly used to obtain other forms of ID,"*[219] which is rightly described as being "*more sensitive than other attribute data."*[220] There is thus an argument that identity providers should be qualified as joint data controllers with GDS and (government) service providers for the set of processing activities leading to authentication.

Assuming GOV.UK Verify embodies a situation of joint controllership between three parties: the identity providers, GDS and the (government) service providers, it becomes problematic to exclude the activities of identify providers or certified companies from the scope of the compliance checks.[221]

More importantly, assuming GOV.UK Verify embodies a situation of joint controllership between the identity providers, GDS and the government service providers, the identification of a distinct legal basis for the processing performed by identity providers arguably becomes a moot point.

Crucially, assuming GOV.UK Verify embodies a situation of joint controllership, this would require revising the allocation of responsibilities between the different parties, despite the fact that eIDAS expressly contains a provision on liability in its electronic identification chapter, i.e. Article 11. Indeed, as mentioned previously the GDPR opts for a principle of joint and several liability in Article 82(4-5) to be read together with Article 26(3).

5. Conclusion

To conclude, this article suggests that due to the way in which the GDPR strengthens both the rights of data subjects (e.g. through granting a right to compensation based upon a presumption of liability), and revisits the status of data processors as well as narrows down the remit of the legal basis based on consent, it will have a considerable impact in the field of electronic identification as in many other sectors. One significant conclusion that can be drawn from this conclusion is, therefore, that data protection impact assessments performed at the time of the DPD should be re-conducted in order to fully take into account the novelties brought about by the GDPR. Critically, the DPIA for GOV.UK

[212] *Ibid*, clause 17.4.
[213] *Ibid*, clause 17.5.
[214] *Ibid*, clause 17.6.
[215] *Ibid*, section F(23).
[216] *Ibid*, section F(22).
[217] *Ibid*, section E(20).
[218] n.**Error! Bookmark not defined.**. pg. 11.
[219] *Ibid*, p. 19.
[220] *Ibid*, p. 19.
[221] *Ibid*, pg. 23. The reason given is that these companies are covered by separate contractual and legal obligations.

Verify, the UK eID scheme, should be conducted afresh as matter of urgency, as its development to date has seemingly been premised upon a DPIA that is now worryingly outdated. As a means of supporting this position, this article has highlighted and analysed several apparent flaws in GOV.UK Verify's DPIA, the most significant and notable of which being the identification of an erroneous selection of legal bases and a set of liability stipulations which would appear to be incompatible with the substantive provisions of the GDPR.

More specifically, the article has argued that identifying the appropriate legal basis for the processing of personal data requires a prior understanding and characterisation of the relationship between the different actors participating in said processing in order to determine whether one legal basis, or perhaps several legal bases, are required, and whether some should be excluded from the very beginning given the involvement of stronger parties, such as public authorities. Furthermore, the characterisation of a situation of joint controllership requires taking a holistic approach to the set of processing activities intended to achieve a specified and/or specific purpose. This is the only way to ensure the full effects of Article 82 of the GDPR.

Finally, the article has argued that, rather than being considered as antagonistic to one another, eIDAS and the GDPR should be seen as complementary pieces of legislation. Both, for instance, are simultaneously sector-specific: eIDAS only applies to electronic identification and trust services, while the GDPR only applies to the processing of personal data. This should mean that when eIDAS and GDPR provisions are potentially in conflict, a detailed analysis of each of their respective apparently conflicting provisions should be undertaken in order to select those that are the most restrictive. This is because electronic identification and trust services are about to become, if they are not already, essential gateways to eGovernment services, and most likely to the Digital Single Market as well.

6. References

'Privacy and Consumer Advisory Group' (*Gov.UK*) <https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group> accessed 9 June 2017

'What is the Government Gateway?' (*Government Gateway Help Desk*) <http://www.gateway.gov.uk/Help/Help.aspx?content=help_more_info_gateway.htm&languageid=0> accessed 20 September 2017

Re Caughey ex p. Ford [1876] 1 ChD 521

Schroeder Music Publishing Co Ltd v Macaulay [1974] 1 WLR 1308

Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein, Case 120/78, [1979] ECR -00649 (EU:C:1979:42)

Bell v Alfred Franks and Bartlett Co Ltd [1980] 1 ALL ER 356

A-G's Reference (No 6 of 1980) [1981] 2 All ER 1057

Barthold v Germany [1985] 7 EHRR 383

A. Foster and others v British Gas plc. , Case C-188/89, [1990] ECR I-03313 (EU:C:1990:313)

Stichting Collectieve Antennevoorziening Gouda and others v Commissariaat voor de Media, Case C-288/89, [1991] I-04007 (EU:C:1991:323)

Innovations (Mail Order) Ltd v Data Protection Registrar [1992] (Case DA/92 31/49/1)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L 281/31

Linguaphone Institute v Data Protection Registrar [1995] (Case DA/94 31/49/1)

Reinhard Gebhard v Consiglio dell'Ordine degli Avvocati e Procuratori di Milano, Case C-55/94, [1995] I-04165 (EU:C:1995:411)

Union royale belge des sociétés de football association ASBL v Jean-Marc Bosman, Royal club liégeois SA v Jean-Marc Bosman and others and Union des associations européennes de football (UEFA) v Jean-Marc Bosman, Case C-415/93, [1995] ECR I-04921 (EU:C:1995:463)

Vereinigte Familiapress Zeitungsverlags- und vertriebs GmbH v Heinrich Bauer Verlag, Case C-368/95, [1997] ECR I-03689 (EU:C:1997:325)

British Gas Trading Ltd v Data Protection Registrar [1998] 1 Info TLR 393, DPT

Aston Cantlow Parochial Church Council v Wallbank [2003] UKHL 37

Criminal proceedings against Bodil Lindqvist, Case C-101/01, [2003] ECR I-12971 (EU:C:2003:596)

Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC [2003] OJ L 41/26

Brian Francis Collins v Secretary of State for Work and Pensions, Case C-138/02, [2004] ECR I-02703 (EU:C:2004:172)

R v Barnes [2004] EWCA Crim 3246

Identity Cards Act 2006, c 15

YL v Birmingham City Council [2007] UKHL 27

'Digests of Approval Profiles for IdP-related Services' (*tScheme*, 2010) <http://www.tscheme.org/profiles/IdP_digest_2.html> accessed 8 August 2017

European Commission v Portuguese Republic, Case C-543/08, [2010] ECR I-11241 (EU:C:2010:669)

European Commission v The Bavarian Lager Co. Ltd., Case C-28/08 P, [2010] ECR I-06055 (EU:C:2010:378)

Identity Documents Act 2010, c 40

Olympique Lyonnais SASP v Olivier Bernard and Newcastle UFC, Case C-325/08, [2010] ECR I-02177 (EU:C:2010:143)

Bonnier Audi AB and others v Perfect Communication Sweden, Case C- 461/10, [2012] (EU:C:2012:219)

Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (Text with EEA relevance) (COM(2012) 238 final, 4 June 2012)

Fish Legal and Emily Shirley v Information Commissioner and Others, Case C- 279/12, [2013] (EU:C:2013:853)

Michael Schwarz v Stadt Bochum, Case C- 291/12, [2013] WLR(D) 386 (EU:C:2013:670)

Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73

Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance) [2015] OJ L 235/1

'Barclays Identity service from Barclays Bank Plc: Grant of Approval' (*tScheme*, 30 June 2016) <http://www.tscheme.org/directory/Barclays/index.html> accessed 12 September 2017

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89

'GDPR will come into force in the UK in 2018, minister confirms' (*Out-Law.com*, 9 November 2016) <https://www.out-law.com/en/articles/2016/november/gdpr-will-come-into-force-in-the-uk-in-2018-minister-confirms/> accessed 10 September 2017

'GDPR will come into force in the UK in 2018, minister confirms' (*Out-Law.com*, 9 November 2016) <https://www.out-law.com/en/articles/2016/november/gdpr-will-come-into-force-in-the-uk-in-2018-minister-confirms/> accessed 15 June 2017

'IDaaS service from Experian Limited: Grant of Approval' (*tScheme*, October 2016) <http://www.tscheme.org/directory/EXPN_IDaaS/index.html> accessed 12 September 2017

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119/1

'Royal Free - Google DeepMind trial failed to comply with data protection law' (*ICO*, 3 July 2017) <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/> accessed 20 August 2017

'UK's Trusted List' (*tScheme*, 2017) <http://www.tscheme.org/UK_TSL/index.html> accessed 8 August 2017

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme", Case C-13/16, [2017] (EU:C:2017:336)

ABC4Trust Position Paper, *Privacy-ABCs and the eID Regulation* (2014) <https://abc4trust.eu/download/documents/ABC4Trust-eID-Regulation.pdf> accessed 03 August 2015

Akman P, *The Concept of Abuse in EU Competition Law: Law and Economic Approaches* (Hart Publishing 2012)

Article 29 Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context* (WP 48, 13 September 2001)

--, *Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC* (WP 90, 27 February 2004)

--, *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995* (WP 114, 25 November 2005)

--, *Opinion 1/2010 on the concepts of "controller" and "processor"* (WP 169, 16 February 2010)

--, *Opinion 15/2011 on the definiton of consent* (WP 187, 13 July 2011)

--, *Opinion 06/2013 on open data and public sector information ('PSI') reuse* (WP 207, 5 June 2013)

--, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217, 9 April 2014)

--, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248, adopted on 4 April 2017)

Black D, 'Validating identity information against an authoritative source' 10 October 2014) <https://identityassurance.blog.gov.uk/2014/10/10/introducing-the-document-checking-service/> accessed 12 September 2017

Blume P, 'Controller and processor: is there a risk of confusion?' (2013) 3 International Data Privacy Law 140

Cabinet Office, 'Government Digital Strategy: December 2013' (*Gov.UK*, 10 December 2013) <https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy> accessed 2 June 2015

--, *Framework Agreement and Schedules* (Draft v0,9, 20 December 2014) <http://data.gov.uk/data/contracts-finder-archive/contract/1690273/> accessed 21 August 2015

--, 'Good Practice Guide No. 45: Identity Proofing and Verification of an Individual' 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf> accessed 12 October 2015

--, *Identity Assurance Hub Service SAML 2.0 Profile v1.2a* (August 7 2015) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/279643/Identity_Assurance_Hub_Service_Profile_v1.2a.pdf> accessed 20 June 2016

Cavoukian A, 'Privacy by Design' (*Information & Privacy Commissioner of Ontario*, 2009) <https://www.privacybydesign.ca/index.php/paper/privacy-by-design/> accessed 27 January 2017

Letter from Denam E,Information Commissioner, to Solma SD (3 July 2017) <https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf> accessed 12 August 2017

Department for Business EaIS, *Electronic Signatures and Trust Services* (Guide, August 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/beis-16-15-electronic-signatures-guidance.pdf> accessed 2 August 2017

Department for Digital, Culture, Media & Sport, 'Collection: Data Protection Bill 2017' (*Gov.UK*, 14 September 2017) <https://www.gov.uk/government/collections/data-protection-bill-2017> accessed 20 September 2017

--, 'UK Digital Strategy 2017' 1 March 2017) <https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy> accessed 8 September 2017

Department for Digital, Culture, Media & Sport and The Rt Hon Matt Hancock MP, 'Government to strengthen UK data protection law' (*Gov.UK*, 7 August 2017) <https://www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law> accessed 16 August 2017

European Commission, *Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market* (COM(2012) 238 final, 4 June 2012)

--, *Feasibility study on an electronic identification, authentication and signature policy (IAS)* (Final Version (D11b), Ref Ares(2013)2869715, 13 August 2013)

--,'Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)' COM/2017/010 final

Government Digital Service, 'Gov.UK Verify Technical Guide' (*Gov.UK Verify Technical Guide documentation*, 2014) <http://alphagov.github.io/rp-onboarding-tech-docs/index.html> accessed 2 June 2017

--, *Gov.UK Verify Data Protection Impact Assessment* (18th May 2016) <https://identityassurance.blog.gov.uk/wp-content/uploads/sites/36/2016/05/GOV-UK-Verify-DPIA-v1.0.pdf> accessed 2 June 2017

Hon WK, Millard C and Walden I, 'Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2' (2012) 2 International Data Privacy Law 3

Hughes J, 'How we're working to increase the range of data sources available for GOV.UK Verify' (*Gov.UK Verify Blog*, 1 December 2014) <https://identityassurance.blog.gov.uk/2014/12/01/data-sources/> accessed 5 August 2017

Comment from -- to Mark (5 January 2016) <https://identityassurance.blog.gov.uk/2015/12/03/working-with-identity-providers-as-they-become-certified-companies/ - comment-41610> accessed 12 September 2017

Identity Assurance Team, *Identity Assurance Documentation* (Release, November 13 2015) <https://media.readthedocs.org/pdf/random/latest/random.pdf> accessed 2 June 2017

Information Commissioner, *Data Controllers and Data Processors: What the Difference is and What the Governance Implications Are* (Guidance, 06 May 2014) <https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf> accessed 7 September 2017

--, *Big data, artificial intelligence, machine learning and data protection* (v 2,2, 4 September 2017) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 20 September 2017

--, *Consultation: GDPR consent guidance* (2017) <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> accessed 23 May 2017

--, *The Guide to Data Protection* (v2,9,5, 7 July 2017) <https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-9.pdf> accessed 20 August 2017

--, *The public interest test: Freedom of Information Act* (v 2,1, 2017) <https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf> accessed 20 September 2017

Klingenberg AM, 'Catches to the right to be forgotten, looking from an administrative law perspective to data processing by public authorities' (2016) 30 International Review of Law, Computers & Technology 67

Knight A, 'CJEU Advocate General Opines on the 'Legitimate Interest' Concept' (*Inforrm's Blog*, 5 February 2017) <https://inforrm.wordpress.com/2017/02/05/cjeu-advocate-general-opines-on-the-legitimate-interest-concept-alison-knight/> accessed 20 September 2017

Kosta E, *Consent in European Data Protection Law* (Brill 2013)

Kuner C, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007)

Lloyd I, *Information Technology Law* (Oxford University Press 2017)

Mäkinen J, 'Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things' (2015) 24 Information & Communications Technology Law 262

Massacci F and Gadyatskaya O, *How to get better EID and Trust Services by leveraging eIDAS legislation on EU funded research results* (White Paper, October 2013, 2013) <http://www.cspforum.eu/Seccord_eidas_whitepaper_2013.pdf>

OECD, *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy* (2011) <http://www.oecd.org/sti/ieconomy/49338380.pdf> accessed 3 August 2017

Olsen T and Mahler T, *Privacy - Identity Management Data Protection Issues in Relation to Networked Organisations Utilizing Identity Management Systems* (LEGAL IST: Legal Issues for the Advancement of Information Society Technologies, Deliverable D11, 2005)

PBLQ, *International Comparison eID Means* (Final report, version 1,0, 10 April 2015) <https://kennisopenbaarbestuur.nl/rapporten-publicaties/international-comparison-eid-means/> accessed 10 September 2017

Privacy and Consumer Advisory Group, *Identity Assurance Principles* (v31, 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/361496/PCAG_IDA_Principles_3.1__4_.pdf> [preserved at: https://perma.cc/5K2W-8BVK] accessed 2 June 2015

Purtova N, 'Between GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships' (2017) [pending] International Data Privacy Law <https://ssrn.com/abstract=2930078> accessed 16 August 2017

Savas ES, *Privatization And Public-Private Partnerships* (Chatham House 2000)

Schermer BW, Custers B and van der Hof S, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16 Ethics and Information Technology 171

Schillig M, 'Inequality of Bargaining Power Versus Market for Lemons: Legal Paradigm Change and the Court of Justice's Jurisprudence on Directive 93/13 on Unfair Contract Terms' (2009) 33 European Law Review 336

Stevens T, 'GOV.UK Verify: privacy and consent' (*Gov.UK Verify Blog*, 30 July 2015) <https://identityassurance.blog.gov.uk/2015/07/30/gov-uk-verify-privacy-and-consent/> accessed 12 September 2017

Tsakalakis N, O'Hara K and Stalla-Bourdillon S, 'Identity assurance in the UK: technical implementation and legal implications under the eIDAS regulation' (Proceedings of the 8th ACM Conference on Web Science (WebSci'16), Hannover, Germany, May 2016) <https://doi.org/10.1145/2908131.2908152> accessed 10 August 2017

Tsakalakis N, Stalla-Bourdillon S and Sel M, *Deliverable 2.7: State of the art in relation to privacy and data protection requirements* (Preliminary report, FutureTrust project [pending], 2017)

van der Sloot B, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307

Van Eecke P and Truyens M, 'Privacy and social networks' (2010) 26 Computer Law & Security Review 535

Williamson-Pound A, 'Becoming a GOV.UK Verify certified company' (*Gov.UK Verify Blog*, 2016) <https://identityassurance.blog.gov.uk/2016/02/25/becoming-a-gov-uk-verify-certified-company/> accessed 2 August 2017

Zwingelberg H and Schallaböck J, *H2.4 The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective* (Opinion Paper, ABC4Trust EU Project, 31 October 2013) <https://abc4trust.eu/index.php/pub/deliverables/176-h2-4> accessed 03 August 2015